Improving Social Maturity of Cybersecurity Incident Response Teams

Acknowledgements

This material is based on research sponsored by the US Department of Homeland Security (DHS) Science and Technology Directorate, Homeland Security Advanced Research Projects Agency, Cyber Security Division (DHS S&T/HSARPA/CSD), BAA 11-02, and the Air Force Research Laboratory Information Directorate under agreement FA8750-12-2-0258. The US government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notation thereon. We acknowledge the contribution of all team members on this research effort.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government.

U.S. Department of Homeland Security
Homeland Security

George Mason University

National Cyber Security Centre
Ministry of Security and Justice

MSB
Swedish Civil Contingencies Agency

Hewlett Packard Enterprise

Dartmouth

Project Team

George Mason University

Lois E. Tetrick, Ph.D.
Stephen J. Zaccaro, Ph.D.
Reeshad S. Dalal, Ph.D.
Julie A. Steinke, Ph.D.
Kristin M. Repchick, M.A.
Carolyn J. Winslow, M.A.
Amber K. Hargrove, M.A.
Tiffani R. Chen, Ph.D.
Tracy C. McCausland, Ph.D.
Alan J. Tomassetti, M.A.
Daniel B. Shore, M.A.
Jennifer P. Green, M.A.
Laura Fletcher, M.A.
Balca Bolunmez, MBA
Zitong Sheng, M.A.
Qikun Niu, M.A.
Aiva K. Gorab, M.A.
Shannon W. Schrader

Dartmouth College

Shari L. Pfleeger, Ph.D.

Hewlett Packard Labs

William G. Horne, Ph.D.
Sandeep N. Bhatt, Ph.D.

Arch Street

Tim Clancy, Arch Street LLC

Document Designed by:

Anastacia Stornetta-Morabito, M.A.

This project could not have been accomplished without the support and participation of our sponsors: United States Homeland Security, Science and Technology, Cyber Security Division; The National Cyber Security Centre, Ministry of Security and Justice, The Netherlands; the Swedish Civil Contingencies Agency. In addition to our sponsors, we wish to thank all of the cybersecurity professionals, their organizations, and managers who participated in various phases of our project. They generously shared their expertise and time to provide valuable insights into the work and structure of cybersecurity incident response teams.

Table of Contents

List of Figures

List of Tables

List of Acronyms

ACM – adaptive case management

CERT – computer emergency readiness team

CEO – chief executive officer

CPS – collaborative problem solving

CSIRT – cybersecurity incident response team

CSIRT MTS – cybersecurity incident response team multiteam system

CTA – cognitive task analysis

DDD – distributed dynamic decision-making

DHS – Department of Homeland Security

HR – human resources

ISACS – information sharing and analysis centers

KSAOs – knowledge, skills, abilities and other characteristics

MSB – Swedish Civil Contingencies Agency

MTS – multiteam system

NCSC-NL – National Cyber Security Centre of the Netherlands

OSPAN – operation word span

PDCA – plan, do, check, and act

PII – personally identifiable information

RPD – recognition primed decision

SBAR – situation, background, assessment, and recommendation

SBT – simulation-based training

SCC – sector coordinating councils

SIEM – security information and event management

SHARED – situation, history, assessment, risks, events, and documentation

SKUE – shared knowledge of unique expertise

SMARTT – situation, management, activity, rapidity, troubleshoot, and talk

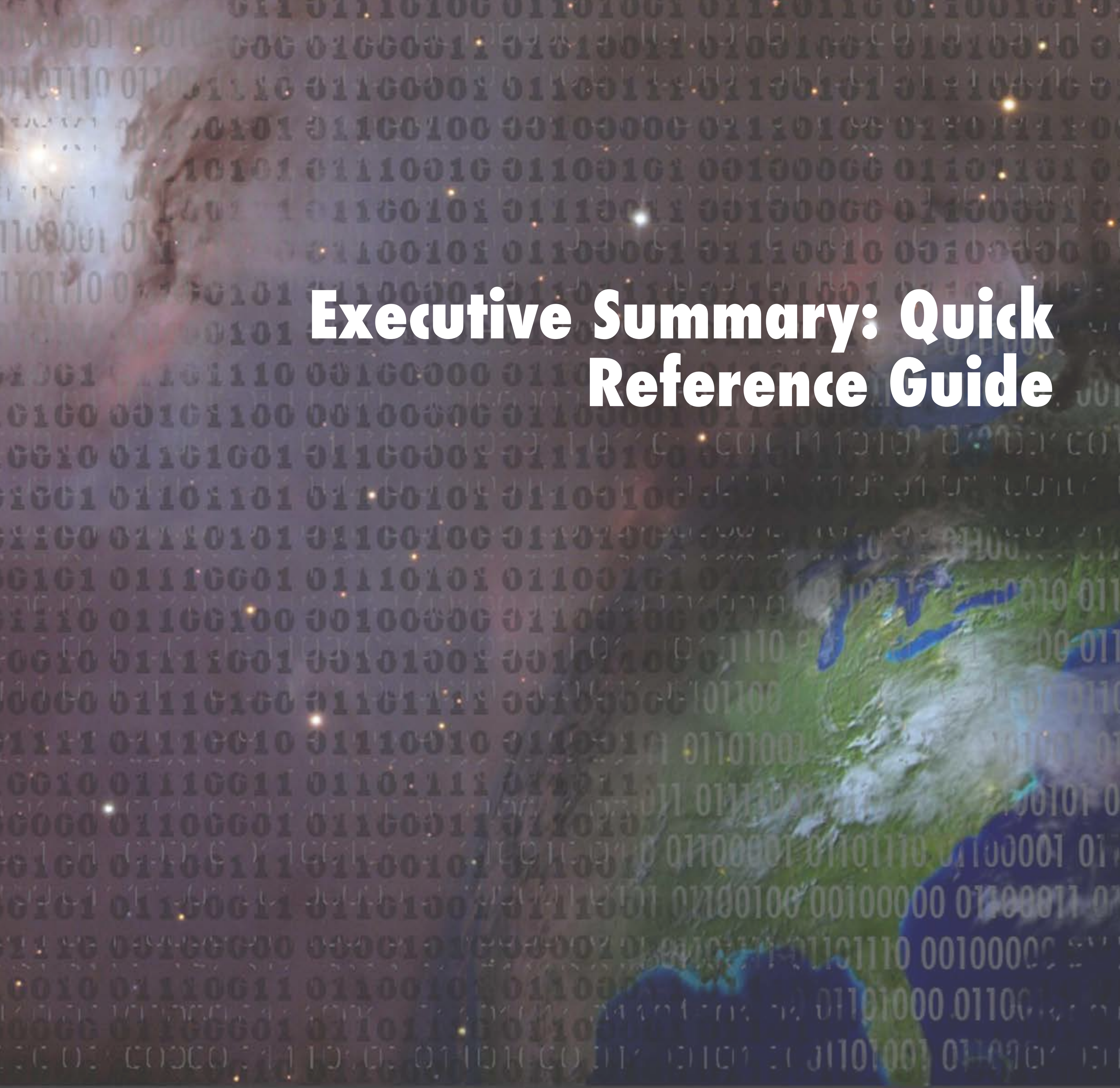
SNAPPS – summarize, narrow, analyze, probe, plan, and select

SOC – security operation center

SSA – sector-specific agency

VUCA – volatile, uncertain, complex, and ambiguous

Executive Summary: Quick Reference Guide



INTRODUCTION

Cybersecurity in the twenty-first century reflects the most technologically sophisticated threat environment the world has ever seen. Cyber incidents are asymmetric and evolving – threatening institutions, individuals, organizations, and governments. The familiar refrains "attribution is difficult" and "the threat is amorphous" have become the stuff of industry lore. In this environment, organizations frequently seek to stay ahead of the threat by maintaining a distinct technological advantage. This advantage has long been accepted as a given considering the history and evolution of the cyber domain. The Western world not only invented the Internet and the systems that form its architecture, but institutions of higher education have responded by producing human talent that is adept at using the latest technologies. Our tools are second-to-none, and our capacity to train people in the use of these tools has never been greater.

Yet, the technological edge enjoyed by organizations in developed nations is diminishing as the world further integrates its knowledge. Furthermore, while technology enjoys pride of place in any conversation on cybersecurity, technology is only part of the solution to real-time cybersecurity. Technology relies upon the people behind it, and because cybersecurity incident response increasingly requires collective action, this creates an entirely new paradigm for cybersecurity. The latest technologies remain bound to human social dynamics and approaches to collective problem-solving that pre-date our species' mastery of fire.

In short, the *ability* to make fire is inconsequential when two people — one holding the steel and the other the flint—are not collaborating.

Today, social dynamics are more important than ever, particularly in the practice of cybersecurity incident response, which requires a well-managed, skilled and efficient Cybersecurity Incident Response Team (CSIRT). For CSIRT managers, finding the right mixture of talent and creating the right social dynamics is both imperative and increasingly challenging. Cybersecurity incident responders often need to work within volatile, uncertain, complex, and ambiguous (VUCA) environments. So much of the counterintuitive skillset that makes a good analyst—creative problem-solving, outside-the-box thinking, and subject expertise—reflects a mosaic of skills that make traditional notions of collaboration challenging.

For managers, building CSIRTs that can maintain tight time constraints and achieve data accuracy, all while working in an evolving threat landscape, will require a renewed focus on team building and collective problem-solving. Such a complex environment, and its many challenges, launched the research that led to this body of work.

STOPPING SOPHISTICATED THREATS REQUIRES SOPHISTICATED TEAMS

The effectiveness of CSIRTs rests on both *technological* and *social* capacities. Both are necessary; neither is sufficient. Yet despite the joint importance of these capacities, most handbooks and training programs designed to increase CSIRT effectiveness focus mainly on technology. When "team" aspects of computer security incident response are addressed in existing work, the emphasis is typically on individual functions and incident response process flow. This Handbook responds to the growing sense among CSIRT professionals that human tech savvy is increasingly not enough; and it is certainly not scalable in lock-step with the outgrowth of cyber threats.

This first-of-its-kind Handbook is written precisely to address this challenge, and, above all, to answer the question: *How does a CSIRT manager assemble and cultivate a team capable of delivering effective cybersecurity incident response?*

What constitutes good performance among cybersecurity incident responders is not well understood. The research summarized in this body of work identified several social processes and dynamics that contribute to incident response effectiveness. *This Handbook, at the most practical level, seeks to provide a baseline for achieving effective CSIRT performance*. It provides the methods and strategies necessary to build, staff, train, and foster a team that leverages both the latest technologies and the social dynamics required to make the best use of them.

A sophisticated, high-performing CSIRT is not just a single team, but rather, a closely connected network of teams. Such component teams are often identified by function within the overall CSIRT, such as forensics or threat intelligence. This network of teams is known as a multiteam system, or MTS. This concept will be emphasized throughout this handbook. When reading these chapters, it is important to keep in mind that building a productive CSIRT requires not just collaboration between individual team members, but collaboration among the component teams as well. The success of a CSIRT can hinge on these MTS interactions: a CSIRT can have strong collaborative bonds within teams, or be well-led overall, but still fail due to mistrust or lack of communication among individual CSIRT component teams.

The dynamic nature of an MTS, in particular, means that CSIRT managers must develop a firm understanding of the social dynamics that drive people in a complex organization. This is especially important when considering that MTSs are the future of cyber incident response and must become as operationally agile as the evolving threat. The Handbook provides several recommendations to address complex MTS challenges including mapping the team relationships within the CSIRT, assessing the social maturity of the overall CSIRT team and the MTS relationships, greater use of situational interviewing and emphasizing common or shared goals among the CSIRT MTS.

USING THIS GUIDE

With an eye towards presenting both a practical tool for CSIRT managers, as well as our team's full research findings, we begin the Handbook with a detailed Executive Summary (Quick Reference Guide). The Quick Reference Guide represents an accessible reference tool for identifying and correcting weaknesses within teams, as well as exercises for improving process flow across a CSIRT. Using the *Quick Reference Guide* will help optimize the performance of individuals, teams and MTSs in cybersecurity incident response.

The *Quick Reference Guide* highlights key findings, recommendations and strategies to help CSIRT managers build the best cybersecurity incident response teams possible. We discuss findings across ***Ten Key Areas*** (click on each for relevant discussion) and, where applicable, offer recommendations for applying these areas to your CSIRT. These key areas are:

1. Social Maturity of Teams
2. CSIRT Performance Evaluation
3. Decision-Making in CSIRTs
4. Communication Effectiveness
5. Information Sharing
6. Collaborative Problem-solving
7. Shared Knowledge of Unique Expertise
8. Trust in Teams and Incident Response Multiteam Systems
9. Sustained Attention and Focus Over Time
10. Continuous Learning in Incident Response

In response to our findings, we have also provided tools for CSIRT managers to help operationalize these findings: a series of Assessment Exercises and Improvement Strategies found in Section 6 at the end of the Guide.

The rest of the Handbook represents the full body of our team's work and a comprehensive compilation of our findings. While the Quick Reference Guide offers a practical tool, the rest of the Handbook provides more insight into the complex social dynamics that undergird cybersecurity incident response. The Handbook examines the ten key areas listed above by chapter, which include extensive explanatory data and supporting documentation for all recommendations and strategies. Links are provided from the Quick Reference Guide to relevant sections of the Handbook for a more in-depth discussion of a particular topic.

CSIRT managers seeking a full understanding of best management practices should familiarize themselves with the full body of work. This is particularly true when making use of the Assessment Exercises and Improvement Strategies. These strategies reflect findings from the most comprehensive study on the social dynamics of CSIRTs to date; however, they are in no way intended to limit novel and future approaches to managing an effective CSIRT. Reviewing the Handbook beforehand will enable managers to more effectively tailor these recommendations and strategies to their needs and objectives.

PROJECT SCOPE

This Handbook was developed as the culmination of a research effort jointly funded by the U.S. Department of Homeland Security (DHS), the National Cyber Security Centre (NCSC) of the Netherlands, and the Swedish Civil Contingencies Agency (MSB). This effort joined scientists from three institutions, George Mason University, Dartmouth College, and Hewlett-Packard, to create a large multidisciplinary research team.

One purpose of our research effort was to examine CSIRT MTSs that are typically used to resolve cybersecurity incidents. Another purpose was to define the planning processes, behaviors, and outcomes that reflect successful CSIRT performance at the individual, team, and MTS level. Several projects comprised our research effort, including:

- **Construction and Validation of an Incident Response Performance Taxonomy**. Our research team developed a taxonomy of cybersecurity incident response performance, which indicates three dimensions of performance: *level* (individual, team, MTS), *timing* (proactive versus reactive processes), and *performance phase* (planning vs. execution activities). We used this taxonomy to derive Knowledge, Skills, Abilities and Other attributes (KSAOs) necessary for effective cybersecurity performance.
- **Review of Existing CSIRT Research**. Our research team undertook a comprehensive review of existing academic and applied research on CSIRT effectiveness, which contributed to the construction of the taxonomy of cybersecurity incident response performance.
- **Review of Existing CSIRT Job Analyses**. In developing a job analysis, our team conducted a study of the cognitive, social, personality, and motivational requirements involved in cybersecurity incident response and then validated our conclusions against several existing analyses in the field.
- **Review of Job Ads for CSIRT Positions**. Our team reviewed over 100 job advertisements for cybersecurity personnel hires and identified (a) the KSAOs typically sought by cybersecurity managers and (b) the gaps between such KSAOs and those attributes identified as important in our research.
- **Focus Group Interviews**. Our research involved one of the most comprehensive sets of interviews of incident responders in a single study. We conducted 52 focus group interviews with a total of approximately 150 participants. We also interviewed 28 representatives of CSIRT MTSs. The interviews included CSIRTs from 17 organizations across the United States, the United Kingdom, Germany, Sweden, and the Netherlands. The types of CSIRTs represented in our sample included government CSIRTs, military CSIRTs, managed security provider CSIRTs, corporate CSIRTs, and academic institution CSIRTs.
- **Survey of Non-Technical KSAOs**. Previous known studies of CSIRTs did not examine cognitive, social, and character attributes that influence CSIRT performance. As part of this effort, we developed a comprehensive list of such attributes from our taxonomy, our focus group interviews, and from a survey of 88 CSIRT professionals.
- **Cognitive Task Analysis**. Most job analyses focus on the behaviors required for job performance. However, because our taxonomy indicated the centrality of

CYBERSECURITY EXAMPLE	AREAS FOR IMPROVEMENT (RELEVANT HANDBOOK CHAPTER/APPENDIX)
Many incidents require collaboration across organizational boundaries. However, information varies according to what data is collected as well as how and with whom it is shared.	• Communication across teams, organizations, and culture (5) • Identify what information to share, with whom and how (6, 11) • Identify performance metrics to evaluate whether CSIRTs successfully collaborate, communicate, and share information (3) • Encourage the development of effective networks and networking skills (11) • Enable CSIRTs to function as a multiteam system (2)
Turnover among CSIRT members can be high due to factors such as lack of preparedness or training, burnout from being overworked, and person-job fit, among others.	• Develop positive individual and team reactions to stress to enhance resilience (Appendix I) • Promote a climate of trust and respect among team members (11) • Increase individuals' ability to sustain attention and focus over long periods of time (9) • Identify appropriate knowledge, skills, abilities, and other characteristics of the job that can be used to select job candidates who "fit" the job (2, 5, 7) • Identify performance gaps that would benefit from training (3)
Policy requirements place restrictions on what and how information can be shared.	• Understand methods of effective communication (5) and their impact on information sharing (6) • Collaborate to solve problems (7) across team or organizational boundaries (2) • Manage conflict based on disagreements about processes (8)
CSIRT members perform at different levels of ability, sometimes due to differences in experience despite similar training.	• Develop a focus on learning among individuals and within the team, MTS, or organization (11)
Difficulty in distinguishing novel incidents from frequent events makes it hard to predict how an incident should be handled.	• Collaborate to solve problems (7) • Increase individual and team capacity to adapt to novel circumstances (7) • Enable CSIRTs to function as a multiteam system (2)
Unusual events require decision-making about whether to collaborate with others to escalate the event to an incident.	• Identify event and incident characteristics that influence decision-making (4) • Collaborate to solve problems (7) • Communicate with others under stressful circumstances (5) • Identify information to share during incident response (6) • Increase interactions with other teams and/or organizations (2)
Workers complete 12-hour shifts on a regular basis and frequently become stressed and irritable during incidents that require more attention over several days or weeks.	• Maintain sustained attention and focus over time (10) • Share incident information through effective communication during shift changes (5, 6) • Preserve individual and team resilience over long periods of time (Appendix I) • Manage conflict that results from work pressure or process disagreements (9)
Analysts tend not to want to request help from other analysts with particular expertise and experiences to collaborate on the resolution of unique incidents.	• Include a focus on an individual's preference for group work in the process for hiring analysts (2) (7) • Develop protocols to determine when analysts should seek help from others (4) • Use training strategies to improve collaboration (7) • Use strategies for developing shared awareness of unique expertise in your team (8) • Use strategies to build trust and psychological safety in your teams (9)
Attempts to collaborate with other analysts or teams with different points of view often result in disruptive conflict.	• Use strategies to build trust and psychological safety in your teams (9) • Employ conflict management strategies to promote constructive exchange of different ideas (9)
Analysts seem unsure about how to respond to unusual events. Delayed responding causes incidents to escalate in severity.	• Develop protocols to determine when analysts should seek help from others (4) • Facilitate use of adaptive case management to facilitate analysts' decision-making processes (4) • Use pre-briefing to develop an understanding among team members about how to respond to unusual events (7) • Use strategies to develop and facilitate adaptive thinking (7)

knowledge work in incident response, we also conducted a cognitive task analysis (CTA) designed to identify the particular cognitive skills that contribute to effective CSIRT performance.

- **MTS Analysis**. As discussed in the introduction, a key aspect our research was to examine CSIRTs as MTSs. Different processes and team dynamics are relevant for MTSs that are not equally relevant for traditional teams. An MTS does not simply refer to a collection of teams working in a CSIRT, but highlights the fact that in CSIRT MTSs, component teams collaborate closely to solve complex problems. This concept in organizational science has been applied to many organizational settings, including military, health, transportation, business, and disaster recovery. We have applied it to the domain of cybersecurity incident response. As part of this effort, we analyzed the elements of 28 incident response MTSs.

FINDINGS AT-A-GLANCE

This section provides a quick snapshot of our findings and what managers need to know to improve CSIRT effectiveness. It is not an exclusive list but is solely for illustrative purposes. For a full discussion please see **Findings and Recommendations** below.

Highlights of Findings:

- Responding to cybersecurity crises is an intense social process.
- Successful cybersecurity incident response requires integration of both technological and social processes.
- Failures in incident response can often be attributed to poor collaboration among team members.
- Cybersecurity incident response often occurs within an MTS, a tightly coupled network of teams that work closely together.
- For individual analysts, curiosity and a preference for working in teams are critical for CSIRT success, but hiring managers often do not recruit candidates based on these attributes.
- Fostering a learning climate across teams, MTSs, and organizations leads to more effective incident response.
- Numerous lessons can be learned from collaboration and team failures in other domains and applied to cyber incidents.

What Managers Need to Know:

- Effective incident response is a complex web of interrelated concepts and strategies spanning 10 key areas. These are highlighted in this Quick Reference Guide and discussed in-depth later on in this Handbook.
- Several "collaboration chillers" can impair CSIRT effectiveness, including:
  1. Failure to share unique information
  2. Failure to initiate necessary collaboration
  3. Failure to adapt
  4. Poor communication practices
  5. Poor listening
  6. Lack of trust
  7. Lack of knowledge about team member expertise
  8. Interpersonal conflict
- Recommended strategies to alleviate collaboration issues and improve CSIRT performance include:
  1. Crafting employee hiring guidelines to focus on critical individual and team characteristics;
  2. Utilization of an Adaptive Case Management (ACM) system to automate processes that otherwise take up valuable time;
  3. Adoption of a balanced scorecard approach to review quantitative performance metrics in a quick yet comprehensive manner;
  4. Emphasizing lower-cost behavioral changes such as regular feedback to and psychological safety for analysts;
  5. Implementing training protocols that emphasize scenario-based practice, role plays, and team simulations;
  6. Greater use of performance aids such as team charters, communication checklists, and managerial guidance; and
  7. Using work design interventions such as work scheduling and physical space to enhance collaboration.
- CSIRT managers can use the assessment exercise found at the end of this Quick Reference Guide, and throughout the Handbook, to determine where their teams need the most improvement and to customize and adapt the strategies most appropriate for them.
- While tailoring for individual circumstances is important, the Handbook also pinpoints common challenges faced by CSIRT managers and makes recommendations based on current research.

FINDINGS AND RECOMMENDATIONS

In this section, we present the ten key areas summarizing our major findings and recommendations.

Social Maturity of Teams. CSIRTs are composed primarily of multiteam systems (MTSs), which are a closely connected network of teams working together to accomplish a common goal. MTSs represent a dynamic and necessary organizational structure for cyber incident response, but MTSs also present complex challenges for CSIRT managers. Our research found that in some instances, when cyber analysts believe they are part of a strong team, they may not as readily trust other teams in the MTS, weakening the MTS as a whole. This frequently requires CSIRT managers to improve communications between teams and identify areas for improvement across the MTS. Conversely, our research also suggests that a strong MTS can often obscure the weaknesses of individual teams. It can actually become more challenging for CSIRT managers to fix the weaknesses of individual teams because the urgency is not as apparent. CSIRT managers must maintain insight into the performance of both individual teams and the broader MTS. Frequently, MTS performance can suffer when teams lack the social maturity to collaborate in the resolution of incidents. Social Maturity is the degree to which a team has the capacity for its members to collaborate in completing the team's mission. Our research found that collaboration can be improved, and team performance can be optimized, when CSIRT managers:

- *Map Their MTS*. This starts with recognizing that their CSIRT is a connected set of teams. It also requires maintaining awareness of both the differing level of interaction between teams, and that these interactions change during higher impact, or more severe, events.
- *Assess the Social Maturity of Each CSIRT Component Team and the Overall CSIRT MTS*. Key team attributes a manager should assess include: collaboration triggering, communication skills and protocols, information sharing, collaborative problem-solving, shared knowledge of unique expertise, trust, adaptation, collective learning, and conflict management.
- *Using Situational Interviews to Make Staffing Decisions and Assess Group Work Preferences*. Managers should ask job candidates a standard set of questions focused on past behaviors and experiences that will illuminate a candidate's ability to work effectively in a group environment.
- *Focus On Emphasizing Distal Goal Commitment*. CSIRT Managers must be advocates for focusing on the goals of the entire CSIRT MTS. Component teams frequently focus on their own goals. CSIRT managers must counteract the tendency by emphasizing common or shared goals.
- *Encourage Regular Cross-Team Connections*. Managers must create opportunities and settings for more communication between different teams.

CSIRT Performance Evaluation. An effective performance measurement and evaluation program can greatly benefit CSIRTs by providing information on individual, team, and MTS behavior that reflect successful job performance. Establishing clear performance metrics can measure the efficiency, effectiveness, value, or impact of an employee's action. Our research found that—especially in light of the diverse composition of a CSIRT and the social maturity required of its teams—performance metrics and evaluation are essential toward constantly improving performance outcomes. A Performance Measurement Program is never static, but our research found that five strategies are instrumental to a successful CSIRT Performance Measurement Program.

- *Balancing Measuring Quantity and Quality*. Quantity falls under objectively-derived metrics, and quality often requires managerial and client ratings. CSIRT managers can use their discretion to determine the balance needed when measuring the quality and quantity of job behaviors; however, the only caution is not to allow metrics alone to guide performance evaluation. Given the imperative of collaboration and communication within an MTS, client ratings can be uniquely useful for CSIRT members.
- *Measure Maximum Performance in Addition to Typical Performance*. In addition to typical performance, which is what managers usually measure, maximum performance can and should be measured through performance on periodically scheduled exercises and simulations. This will allow managers to understand the extent of their team's capabilities.
- *Measure Both Proactive and Reactive Performance*. Every CSIRT manager to whom we spoke confirmed that an appreciable portion of CSIRT tasks involved proactive behavior. Yet, most CSIRTs often skew measurement to reactive performance. Managers should therefore supplement reactive performance metrics with proactive performance metrics.
- *Determine the Appropriate Level of Measurement*. The purpose of measuring performance should guide a CSIRT manager's approach. If the manager wants to determine the strongest and weakest members of a CSIRT, the individual level is most appropriate. If a manager wants to identify strengths and weaknesses of teamwork, the team or MTS level is most appropriate.
- *Create a Balanced Scorecard for Performance Measurement*. Our research found that one tool that can help a CSIRT manager maintain a comprehensive approach to performance measurement is known as the balanced scorecard. The balanced scorecard is not only a dashboard of metrics to measure performance, but it can also suggest the relationship between different categories of performance.

Decision-making in CSIRTs. Our research found that for every incident response trigger, there is an initial decision regarding whether to tend to the event. If the decision is made to act rather than categorize as a false positive, there are numerous subsequent decisions that must be made, including how to prioritize the event. Also, analysts must decide when it is appropriate to call on others to collaborate in order to mitigate the incident (referred to as collaboration triggering). Analysts must know when initiation of collaboration is necessary and when it is unnecessary, such as when the incident is routine. The effectiveness of these decisions depends upon a cybersecurity analyst's abilities. Our research found strategies for improved decision-making.

- *Selecting for Decision-making Skills*. CSIRT Managers should select applicants for their decision-making skills, particularly those involving problem sensitivity, critical thinking, and information ordering. Chapter 4 of this Handbook includes questions to facilitate this selection.
- *Training Decision-making Skills*. We found that structured troubleshooting, critical thinking training, and expert modeling can alleviate the weaknesses in a novices' decision-making. Expert modeling in particular—which pairs a novice with an expert to resolve an incident unfamiliar to the novice—can improve the novice's abilities and team performance.

- *Cognitive Prompts for Expert Analysts*. Cognitive prompts can reduce overconfidence and information bias. One such strategy is the “Five-Why Analysis,” developed by Toyota and used widely by a range of companies including Amazon.com. It involves asking “Why?” a particular incident happened and applying the same question five times to each answer. In cybersecurity, five-why analysis is believed to be more effective for use by teams of cybersecurity analysts rather than individual team members. Another strategy, “the premortem,” asks analysts to imagine they have already attempted to resolve the incident but have failed. They are then asked to identify the reasons why the incident response effort may have failed.
- *Using Mnemonics to Capture Necessary Information*. Mnemonics facilitate the use of protocols that remind the decision-maker to consider different aspects of a new situation. A widely used mnemonic in healthcare is SBAR, which stands for Situation, Background, Assessment, and Recommendations. SBAR has been shown to improve the communication of patient information among healthcare staff in a number of studies.
- *Using Adaptive Case Management*. In contrast to process models, an adaptive case management system focuses on the individual case—that is, the incident. Rather than prescribing general processes that the analyst is expected to follow, an ACM system provides context surrounding the incident by summarizing the ways in which similar incidents were handled in the past and the extent to which those ways proved successful.

Communication Effectiveness. Our study found that cybersecurity analysts rated communication skills at the top of social skills needed for CSIRT effectiveness. Three common challenges to communication effectiveness in CSIRTs include time demands, team member physical distance, and the need to communicate across cultural boundaries. To promote communication effectiveness, CSIRT managers need to ensure messages are clear in meaning, relevant in content, as well as appropriately timed, sent to the correct person, and acknowledged by recipients. Effective communication serves as a foundation for information sharing across individuals, teams, and MTSs.

- CSIRT managers can improve communication in their teams and multiteam systems by using aids such as communication charters, handoff checklists, virtual displays, and wikis.
- CSIRT managers can facilitate use of communication aids through scenario-based practice exercises and team simulations.
- CSIRT managers can enhance communication between teams by designating a specific person for each component team responsible for such communication.
- Careful design of physical workspaces can facilitate more frequent communications and sharing of information with appropriate stakeholders.

Information Sharing. Information sharing, in the realm of cybersecurity reflects the exchange of incident knowledge and threat data across and within organizations. The *type* of information shared, *with whom* information is shared, as well as both the *speed* and *accuracy* by which information is communicated before, during, and after an incident help determine the quality of responses to both familiar and novel incidents. Focusing on parameters of information sharing enables managers to identify effective strategies for improving CSIRT processes and performance. As examples, our research found that mandatory information sharing regulations should clearly define *how much of what type of communication should be communicated by when and to whom*. Managers should not discourage the discretionary sharing of information, as such activities promote collaboration. Managers also need to establish specific communication protocols based on various levels of information sharing (e.g., two individuals, within-team, intra- or inter-organizational); different strategies for improving information sharing might work at one level but not at another level. When individual-to-individual information sharing occurs, confirmation and response is fairly straightforward. However, when an individual sends information to an entire team, MTS, organization, or outside organization, responsibility for confirmation and response might not be clear.

To facilitate information sharing, CSIRT managers need to establish communication protocols and charters that do the following:

- Identify the recipients who would most benefit or require the information being shared;
- Consider carefully what information and how much recipients need in order to accomplish their work;
- Set norms for review of information posted for accuracy and completeness;
- Specify communication methods that allow confirmation of receipt to ensure information was received;
- Provide sender contact information, along with an invitation to request additional information, if necessary;
- Set communication norms within teams that support sharing of discretionary information:
    - When in the incident response cycle information should be sent;
    - What information is necessary for recipients;
    - When particular types of information are needed by others;
    - What types of information are necessary to share during high impact events;
    - How much information is sufficient to create situational awareness.
- In the case of mandatory information sharing, have regulations that clearly define *how much of what type of information should be communicated by when and to whom*:
    - Managers should revise the regulations and protocols that determine the mandatory sharing of information if they receive reports that information being sent

under specific rules is consistently incomplete, irrelevant, inaccurate, not timely, or sent too infrequently (or too frequently).

- In the case of information sharing between individuals, teams, MTSs, organizations, or external stakeholders:
  - Define what kinds of information need to be shared with each.
  - Establish guidelines about which members within a team should respond to which kind of information sent to the entire team (based on knowledge).
  - Establish boundary spanners, or individuals tasked with responding when information sharing occurs between teams in an MTS or between organizations.

Managers should use guided simulations and scenarios to practice the use of these communication charters and protocols to develop a shared understanding within the CSIRT of how information sharing at multiple levels should occur.

Collaborative Problem-solving. The nature of CSIRT work is knowledge work that typically involves multiple team members working together to solve complex problems. CSIRTs must be able to engage in the processes of situational awareness, collective information processing, and forecasting, in order to be effective in solving novel problems. Our research found that managers can improve these processes using strategies such as pre-briefing, debriefing, simulations, and giving focused feedback. Our interviews with CSIRT analysts and managers consistently indicated a higher percentage of endorsement of collaborative problem-solving steps between teams versus within teams, which supports our broader research finding that CSIRTs are often MTSs, conducting problem-solving as closely-knit interdependent teams. Further, our survey of critical knowledge, skills, abilities and other attributes that contribute to effective incident response indicated two problem-solving skills were in the top 10 highest rated attributes. Skill in reviewing information to develop and implement solutions to complex problems ranked fifth highest in importance, and skill in working with other members to solve problems and come to solutions that will help the team ranked tenth highest.

- ***Strategy One:*** *Engage in pre-mission planning (or "pre-briefing").* CSIRT members cannot resolve an incident if they cannot define the problem parameters. Managers should lead a pre-briefing to create a shared understanding of the problem, a shared understanding of the goal or desired outcome, and a shared understanding of the solution strategy. Contingency planning—a variation of pre-briefing—can help teams and CSIRTs anticipate unexpected events by planning how they will be handled in advance.
- ***Strategy Two:*** *Use counterfactual thinking to get team members to share their unique information*. Team members often do not realize that they have information no one else knows. Managers should ask their team members to consider what might have happened in a past situation or a given scenario that is different from what actually happened. This often elicits unique information that individuals would not otherwise share in a group dynamic.
- ***Strategy Three:*** *Provide team feedback during structured debriefing*. After incidents occur, and even after simulations, feedback during debrief is extremely important. It has been shown to improve team performance 19% more than teams who did not receive feedback. Managers or facilitators who are responsible for providing feedback should focus on teamwork successes as well as failures.
- ***Strategy Four:*** *Develop adaptive thinking by providing exploratory or active learning experiences with wide problem variety*. Managers can use forms of exploratory or active learning to develop adaptive thinking skills. Managers should encourage team members to change how they are thinking about a particular problem by using such frame-changing prompts as "How is this problem different from other problems you faced?" or "What other possible solutions might apply to this problem?"
- ***Strategy Five:*** *For MTSs, train leaders to pre-plan strategies for how multiple teams will work together*. Multiteam problem-solving can also be improved using the pre-planning strategies discussed earlier. Team leaders in an MTS can work together to engage in pre-planning that maps out (a) how multiple teams will work together, and (b) how each of those teams will coordinate their actions with other specific teams.
- ***Strategy Six:*** *When staffing, build your CSIRT with team members who have a team orientation and teamwork skills*. A well thought out staffing plan can increase the effectiveness of team collaboration and collective problem-solving. Having high levels of team skills such as cooperativeness, team orientation, and organization skills will enable the team to build the levels of trust and SKUE (shared knowledge of unique expertise) that will foster effective collaborative problem-solving.

Shared Knowledge of Unique Expertise. By necessity, CSIRTs need a diverse collection of members with different perspectives and expertise to respond to ever-evolving incidents. This makes shared knowledge of unique expertise (SKUE) vital for CSIRT operations. Called "transactive memory" by some, SKUE reflects the idea that all CSIRT team members and MTS components must possess the same knowledge of "who knows what" to work efficiently. SKUE decreases the time it takes for CSIRT members to identify who has the knowledge that is needed, resulting in more effective collaboration. In 80% of the focus groups we conducted, knowing who had what expertise on the team was among the most important team attributes for CSIRT effectiveness. Knowing what other members across component teams know quickens the incident response process, including the identification and mitigation of threats. We found that two strategies in particular could help optimize SKUE in CSIRTs.

- ***Strategy One:*** *Establish knowledge tools (e.g. information board, knowledge map) that display members' expertise, knowledge, skills and experiences.*
- ***Strategy Two:*** *Train team members in areas other than their*

specialty. Training team members in roles outside of their own job position is known as cross-training. The three different forms of cross-training are (a) Lecture/ Presentation, which involves a team member communicating or presenting to others aspects of their functional roles and responsibilities; (b) Job Shadowing, which involves team members, particularly novice members, shadowing a more experienced team member; and (c) Position Rotation, which involves individuals temporarily assuming the roles of other team members.

Trust in Teams and Incident Response Multiteam Systems. The CSIRT community has placed a significant emphasis on trust as an important factor for collaboration in incident response, one that was confirmed by our project findings. CSIRTs with high levels of trust facilitate faster threat mitigation with better, more novel solutions due to the conditions created by team leaders. For CSIRTs, trust can exist at multiple levels, including (a) Trust between CSIRT members; (b) Trust between CSIRT leaders and subordinates; (c) Trust between teams in an CSIRT MTS; and, (d) Trust between organizations. Our findings have concluded that a series of exercises can be used by CSIRT managers to build trust in their teams, MTSs, and between organizations.

- ***Strategy One:*** *Provide structured opportunities for CSIRT members to learn about the expertise, experiences, and functional backgrounds of other members*. When CSIRTs are newly formed, or when members have not previously worked together, building perceptions of shared competence is an important first step in developing team trust. Disclosing unique skills and experiences related to these roles demonstrates that all team members are competent in their roles and can be counted on to perform tasks. Managers should encourage team members to engage in frequent interaction and information conversations where they exchange information about the following: backgrounds, work experiences, and (some) personal information that emphasizes shared goals and interest in establishing a good relationship.
- ***Strategy Two:*** *Establish clear individual and team goals, roles, and performance standards.* Developing perceptions of shared competence requires managers to set clear team goals and ensure that members have a clear sense of team goals, their roles in meeting these goals, and the performance standards that indicate goal accomplishment. This will foster increased dependability and reliability within the team. In addition to considering the use of a chartering strategy and pre-briefing, managers should also clearly define team goals for a specific period of time (e.g. monthly) and ask each member to provide a list of goals. Based on team goals, each team member should specify their individual goals and demonstrate alignment with the team's mission. Managers should meet with the team on a regular basis to remind the team of goals, evaluate progress and provide feedback.
- ***Strategy Three:*** *Establish norms for communication transparency in team.* The first two strategies in this section help establish swift trust and establish the basis for further trust development. Deeper levels of trust begin when managers create and enforce a climate for communication transparency. Team members look to the leader for expectations of how they should behave. If CSIRT managers model openness and honesty in their communications with others, then their subordinates will be more likely to do the same. Managers should also enforce a norm for communication transparency by reacting swiftly to violations of this norm. If team members display a reluctance to be open in their interactions with their colleagues, managers should have a "clearing the air" meeting with those particular individuals, with team leads, or, if necessary, with the CSIRT as a whole. The tone of such meetings should be constructive and supportive, with the purpose of addressing issues that are fostering careful disclosure rather than transparency in communications within the team.
- ***Strategy Four:*** *Utilize managerial actions that create a psychologically safe climate in the team.* When CSIRT managers create a psychologically safe climate, team members are more likely to generate novel ideas, explore new perspectives, and learn from mistakes. To create a psychologically safe climate, CSIRT managers should ensure that team members feel valued. They should encourage them to generate the novel ideas that are often necessary to resolve unusual incidents. Creating this atmosphere requires CSIRT managers to take time during meetings to invite all team members to offer opinions, as some might be hesitant to go against the majority. It is important for all team members to be present when discussing important information, to demonstrate inclusivity. Managers should also actively try to take on other team members' perspectives and weight all ideas equally to consider each opinion before coming to a decision. During this process, it is important to encourage team members to bring up difficult topics and reward them (e.g. with praise) for offering new solutions or ideas. Above all, a CSIRT manager must display non-defensive responses to questions and challenges.
- ***Strategy Five:*** *Create opportunities for building strong social connections among CSIRT members to support conflict management.* Both swift trust and deep trust emerge from positive social relationships among CSIRT members. Conflict will always occur in CSIRTs. Yet, a manager can minimize the damage to trust that conflict can cause by helping the team develop stronger interpersonal ties early in the team's formation. This can be as simple as providing "ice-breaking" social activities early in the team's formation or as new members join. Managers should have regular team social activities (e.g. team lunches, gaming activities), especially if the team is not new. Engaging the team (or multiple teams in an MTS) in training activities

that improve conflict resolution will prime the CSIRT to handle conflict constructively when it arises.

- ***Strategy Six:*** *Increase external connections and social networking to facilitate inter-team and inter-organizational trust*. Inter-organizational trust can be built through consistent networking across organizational boundaries, which is key to enhancing CSIRT maturity. This level of networking can be done at annual professional meetings or regularly scheduled meetings among individuals from different organizations who need to work with one another.

Sustained Attention and Focus Over Time. CSIRTs benefit when watch teams are vigilant and able to sustain attention throughout their shift, reducing the occurrence of missed critical events. Our interviews of cybersecurity professionals indicated that employees sometimes look for critical events over extended periods of time (e.g., "eyes on glass"). This runs into the cost-benefit question of sustaining attention versus the quality of work. Frequently, the longer one focuses on a single task the better the achievement of the goal, provided that sustained focus does not compromise cognitive endurance (e.g., fatigue). To improve sustained attention and focus over time, managers should implement as many of our recommended strategies as possible. However, some strategies might not be applicable to specific CSIRTs or might be too costly to implement. For instance, if shift lengths, rotations, and length of breaks cannot be changed, managers could nonetheless provide suggestions for employees regarding the best use of rest breaks (incorporating socialization, for example). Additionally, managers could select employees based upon their ability to sustain attention; however, managers first must validate employee selection tools to ensure that working memory and brief sustained attention (i.e., vigilance) tasks predict sustained attention in CSIRT employees. Managers need to determine the primary factor influencing employees' performance, such as whether employees come to work tired or lose steam throughout work shifts. Shift-length and shift-rotation decisions are useful strategies to address employee fatigue whereas rest-break strategies address decreases in attention over the length of a work shift. All of these factors impact effective cybersecurity incident response, particularly during critical times that require sufficient attention and cognitive endurance.

- ***Strategy One:*** *Hire job applicants who display a capacity for sustained attention*. One way to maximize employee attentiveness is to hire individuals who are better able to sustain attention and focus throughout their shifts. Selecting employees with higher levels of attention could be particularly beneficial for those teams whose tasks predominantly include surveillance tasks, such as monitoring and watch teams. It is difficult to predict individual differences in sustained attention using measures of personality or intelligence. We suggest managers use an employee selection test. Two measures, in particular, could prove useful in predicting an employees' sustained attention throughout their work shift. The first is a "working memory task," which measures the portion of memory that allows temporary storage of verbal or visual information. The second measure involves "brief sustained attention tasks." Performance on these tasks can predict employees' performance on longer sustained attention tasks, such as the monitoring task involved in incident response.
- ***Strategy Two:*** *Encourage employees to incorporate rest breaks into their shifts.* Our interactions with CSIRT members pointed to the importance of periodic rest breaks during the workday. This strategy is practiced among cybersecurity professionals in Europe where a periodic break is endorsed, most often a coffee break. We propose that organizations and managers should provide suggestions to employees about how to incorporate rest breaks into their schedules and encourage employees to take more consistent and regular rest breaks. CSIRT managers should encourage employees to take approximately one 15-minute break every two hours. Managers should also allow employees some latitude regarding when to take breaks, rather than forcing adherence to a rigid break schedule. A rigid break schedule can result in increased emotional strain for employees, possibly resulting from employees being interrupted in the middle of complex tasks. To provide a truly restorative setting during breaks, *natural settings* have been found to contribute to the replenishment of attention. Researchers found that reaction time became faster and attention increased when participants were exposed to a picture of nature compared to pictures of urban scenes. Additionally, socialization can be important to rest breaks. Informal interactions between employees can be a source of stimulation and variety in the work environment.
- ***Strategy Three:*** *Shift Design—Create a shift plan that reduces sleep disturbances and maximizes attentiveness.* Our interviews with cybersecurity professionals demonstrated that shift lengths (e.g., 8-hour vs. 12-hour shifts) and shift rotations (e.g., morning > afternoon > night > morning vs. morning > night > afternoon > morning) differ across CSIRTs. Shifts should be implemented in a way that minimizes sleep disturbances and fatigue among employees. To improve sustained attention, managers should try to schedule employees for 8-hour work shifts as opposed to 12-hour shifts. Managers should seek to implement "rapid shift rotations," where possible. Shift rotation implies that shifts change based on a set schedule, and shift rotation speed refers to the number of consecutive work shifts until an employee's shift changes (e.g., the start and end time of the shift changes). Managers should use rapid shift rotations to increase employee alertness and reduce fatigue. This requires changing shifts every week or couple of days rather than after several weeks. A final critical consideration in shift design involves "shift rotation direction." Shifts typically rotate in a forward or backward direction. When possible, managers should

use forward shift rotations (i.e., morning > afternoon > night > morning) rather than backward shift rotations (i.e. morning > night > afternoon > morning). Research indicates that people acclimate more easily to time zone changes that move clockwise or westward.

Continuous Learning in Incident Response. A continuous, positive learning environment is essential in cybersecurity incident response. CSIRTs are fast-moving. Analysts face rapidly changing threats and respond to increasingly novel situations. To keep pace, CSIRT analysts must utilize their individual inventiveness, and managers need to create systems and institutions that harness this ingenuity. This dynamic demands that cybersecurity analysts and teams constantly learn new skills. Such learning must occur across all levels: individual, team, and MTS.

Learning is not limited to individual skill development. CSIRTs need to place a high value on stored knowledge and must reach collective understandings of constantly evolving conditions. Individual team members and component teams often must adapt by changing their behaviors or worldviews. Managers can foster this process by establishing a trusting environment where individual team members feel confident to share their ideas. Our research has found four key strategies to create a positive learning environment within CSIRTs.

- ***Strategy One:*** *Selection of individuals who are creative and curious.* Curiosity results in information seeking and leads to learning, while creativity leads to explorations of novel directions and modifying and extending known solutions. Hiring people who are creative and curious is one approach for improving those attributes in a CSIRT. The selection of job applicants could be based on previous experience, structured interview questions, or responses to a psychological test.
- ***Strategy Two:*** *Leader behaviors to encourage learning*. Leaders have the ability to encourage creativity and curiosity behaviors. One of the managers we interviewed indicated that he deliberately assigned analysts to work on special development projects, allowing them to show their creativity. Managers can also encourage CSIRT professionals to self-assess their own skills and knowledge. Based on self-assessment, they can plan their own learning activities, which can lead to increased confidence and better performance. Managers who encourage employees to establish goals and development opportunities create a feedback-seeking environment. This creates the opportunity to reward employees for learning new skills. Self-assessment and goal creation is also useful for *teams*. Managers should encourage teams to reflect on events and identify where changes are needed by holding debriefings, also referred to as after-action reviews.
- ***Strategy Three:*** *Design work to enhance learning and development*. Work design refers to the organization of an employee's total role within a team. It can include the job tasks they perform, other activities they may engage in, relationships with others relevant to getting their jobs done, and the responsibilities in accomplishing their overall role. Work design has been demonstrated to affect workers' motivation as well as their learning and development. Research has shown that allowing CSIRT analysts autonomy over their working methods and pace of work can improve performance. Managers should design cybersecurity work roles around tasks that use a variety of skills, which has been shown to increase job performance. One of the most important factors in promoting learning is to put in place mentoring programs, which can help CSIRT professionals identify networking and learning opportunities.
- ***Strategy 4:*** *Development of professional networking skills*. CSIRT managers should help their employees develop networking skills, which aid developmental growth. There are three factors to be considered in establishing a professional network for developmental purposes: (1) Assessment, where members in the network can provide relevant information and feedback on their developmental progress; (2) Challenge, where members of the network can get individuals to move beyond their comfort zones; and (3) Support, where members of the network can provide support, helping individuals manage the challenges faced in increasing their knowledge, skills, and abilities. Managers can also facilitate guided discovery learning. Instead of traditional learning approaches (e.g., lectures, videos, or manuals), in discovery learning workers construct their own understandings through experimentation and exploration. Managers can facilitate discovery learning using the examples in Chapter 11 (Continuous Learning in Incident Response). Lastly, error management training can be a useful mechanism for CSIRT managers to increase team members' comfort with admitting to and learning from mistakes.

TOOLS FOR CSIRT MANAGEMENT—ASSESSMENT EXERCISES & IMPROVEMENT STRATEGIES

Our team prepared the following Assessment Exercises and Improvement Strategies to assist CSIRT managers in evaluating and improving their teams. They are organized by chapter as found in this Handbook. Developed in response to this study's key findings, these questions should serve as prompts for a manager to gain insights into their team's functionality and effectiveness. The Improvement Strategies reflect our recommendations for improving team performance. Our research found common themes, gaps, opportunity costs, and areas for improvement across CSIRTs. While each of the Improvement Strategies may help CSIRTs and CSIRT MTSs, the strategies denoted with a star represent our team's highest recommendations. For each improvement strategy, links are provided to the relevant Handbook chapters that give in-depth descriptions and context.

CHAPTER 3: MEASURING AND EVALUATING CSIRT PERFORMANCE

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. I consider not only conventional, objectively-derived performance metrics, but also subjectively-derived (e.g., using ratings) performance metrics..
2. I consider not only the quantity of performance, but also the quality of performance.
3. I consider not only how well an analyst performs under normal operating circumstances (i.e.,"typical" performance), but also how he or she performs when confronted with very serious incidents (i.e.,"maximum" performance).
4. I consider not only performance after an incident is detected (i.e., reactive performance), but also performance that occurs before an incident is detected (i.e., proactive performance).
5. I consider not only performance at the individual level, but also performance at the team level or other levels (performance at the broader multiteam system level).
6. I consider not only conventional performance outcomes, but also psychological (e.g., well-being) outcomes.

IMPROVEMENT STRATEGIES

Strategy 1: Balance Measuring Quantity and Quality

Strategy 2: Measure Maximum Performance in Addition to Typical Performance

Strategy 3: Measure Both Proactive and Reactive Performance

Strategy 4: Determine the Appropriate Level of Measurement

★ Strategy 5: Create a Balanced Scorecard of Performance Measurement

DECISION-MAKING IN CSIRTS (CHAPTER 4)

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. Analyst expertise is considered explicitly when analysts are assigned (or assign themselves) to incidents.
2. Incident severity is considered explicitly when analysts are assigned (or assign themselves) to incidents.
3. Decision-making skills are emphasized in analyst training activities.
4. My analysts consider all necessary information before they make decisions in response to an incident.
5. My analysts comprehensively rehearse their response plans (including mentally testing them for ways in which they could go wrong) before implementing them.
6. When hiring new analysts, decision-making skills are emphasized.
7. My analysts decide correctly that they should include other analysts in their incident mitigation efforts.
8. Members on my team are proactive, soliciting help from team members.
9. My team solicits help proactively from other teams in the CSIRT MTS.
10. My team asks other teams in the CSIRT MTS to help them resolve an incident when such help is necessary.
11. My team takes the initiative when deciding to include other teams in a CSIRT MTS in their incident mitigation efforts.

IMPROVEMENT STRATEGIES

Strategy 1: Selecting for Decision-Making Skills

Strategy 2: Training Decision-Making Skills

Strategy 3: Cognitive Prompts to Reduce Overconfidence and Confirmation Bias

★ Strategy 4: Using Mnemonics to Capture Necessary Information

★ Strategy 5: Using Adaptive Case Management

COMMUNICATION DURING INCIDENT RESPONSE (CHAPTER 5)

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. Messages sent among my team members contain all critical information.
2. Messages sent or received by the team are understood clearly.
3. My team members ask for clarification for messages received from others when they are unsure of something.
4. My team members confirm receipt and understanding of critical communications.
5. Information is received on time when trying to address a cyber threat.
6. Messages are sent to the correct recipient during different phases of incident resolution.
7. Complete and accurate information is passed during handoffs between different individuals in my team.
8. My team members quickly resolve communication issues with individuals on their teams.
9. My team members quickly resolve communication issues with team members from other cultures.
10. Messages sent between teams in the CSIRT MTS contain all critical information.
11. Different teams ask for clarification for messages received from other teams when they are unsure of something.
12. Confirmation of receipt and understanding of critical communications occurs between teams.
13. Complete and accurate information is passed during handoffs between different teams.
14. Teams quickly resolve communication issues with other teams.
15. Teams in the CSIRT MTS designate a point person to communicate with other teams or external parties.

IMPROVEMENT STRATEGIES

★ Strategy 1: Communication Charters

★ Strategy 2: Handoff Checklists

★ Strategy 3: Scenario-based Practice with Pre-briefing

★ Strategy 4: Team Simulation Training

Strategy 5: Virtual Displays

Strategy 6: Wiki Best Practices

Strategy 7: Boundary-Spanner Designation

Strategy 8: Work Space Design

Strategy 9: Situational Interviews to Select People with Communication Skills

COLLABORATIVE PROBLEM SOLVING (CHAPTER 7)

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. Team members in my CSIRT solicit help from each other proactively.
2. My team members get together to brainstorm and to consult each other about incident resolution.
3. My team members use the knowledge they have gained from other team members in resolving a novel incident.
4. My team members work together to determine the potential consequences of an event or threat to the cybersecurity of the organization or to constituents.
5. Members of my CSIRT consider multiple viewpoints when resolving an incident.
6. Members of my CSIRT are willing to switch to new kinds of solutions when existing ones may not be the best.
7. Members of my CSIRT try new ways of thinking about novel events and incidents.
8. Members of my CSIRT adopt new ways of resolving incidents.
9. Members of my CSIRT are comfortable deviating from normal or typical ways of resolving incidents.
10. My team members change their behaviors or protocols as a result of previous incidents.
11. Members of my team are likely to try new ideas and solutions when resolving incidents.
12. My team members incorporate the expertise of other teams into incident resolution.
13. Teams in my CSIRT MTS solicit help from other teams proactively.
14. Multiple teams get together to brainstorm and to consult each other about incident resolution.
15. Multiple teams work together to determine the potential consequences of an event or threat to the cybersecurity of the organization or to constituents.
16. Teams in the CSIRT MTS change their ways of interacting with one another as a result of previous incidents.

IMPROVEMENT STRATEGIES

★ Strategy 1: Engage in pre-mission planning (or pre-briefing) for teams or MTSs
★ Contingency Planning for teams and MTSs

★ Strategy 2: Use a counterfactual thinking approach to get team members, and teams in an MTS, to share their unique information

★ Strategy 3: Engage teams and MTSs in structured debriefing with feedback

Strategy 4: Develop adaptive thinking by providing exploratory or active learning experiences with wide problem variety

★ Strategy 5: Train leaders to pre-plan strategies for how multiple teams will work together

Strategy 6: Staff your CSIRT with team members who have a team orientation and teamwork skills

SHARED KNOWLEDGE OF UNIQUE EXPERTISE (CHAPTER 8)

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. My team members know exactly who has the knowledge to handle a particular incident.
2. My team members can explain "who knows what" within the team.
3. Members of my team ask the right person for information.
4. In team meetings, members appear to know what other people within my team know.
5. Members of my team communicate what knowledge they possess to other team members.
6. My team members know exactly which team has the right knowledge/expertise to handle a particular incident.
7. My teams explain "which teams know what" within the CSIRT MTS.
8. Members of my team ask the right team in a CSIRT MTS for information.
9. Members of my team communicate what knowledge they possess to other teams in the CSIRT MTS.

IMPROVEMENT STRATEGIES

★ Strategy 1: Knowledge Tools

★ Strategy 2: Presentation (type of cross-training)

★ Strategy 3: Job Shadowing (type of cross-training)

Strategy 4: Position Rotation (type of cross-training)

TRUST AND PSYCHOLOGICAL SAFETY (CHAPTER 9)

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. My team members feel confident about the competence of other members.
2. My team members feel comfortable relying on each other when resolving tough incidents.
3. My team members feel comfortable admitting mistakes or seeking advice without worrying about being judged or evaluated.
4. My team members share learning opportunities with other members.
5. My team members talk freely with each other about difficulties they are having with incidents.
6. My team members bring up tough problems and issues with each other.
7. Members of my team manage differences of opinion without creating tension.
8. Members of my team resolve disagreements about incident mitigation.
9. Members of my team are comfortable having debates about different approaches to incident mitigation.
10. Tension and anger are well managed among members of my team.
11. My team feels confident about the competence of other teams in the CSIRT MTS.
12. My team members feel comfortable relying on other teams in the CSIRT MTS when resolving tough incidents.
13. My team members share learning opportunities with members of other teams in the CSIRT MTS.
14. Members of my team talk freely with members from other teams in the CSIRT MTS about difficulties they are having with incidents.
15. Team members bring up tough problems and issues with members of other teams in the CSIRT MTS.
16. My team manages differences of opinion with other teams in the CSIRT MTS without creating tension.
17. Tension and anger are managed well between teams in the CSIRT MTS.

IMPROVEMENT STRATEGIES

Strategy 1: Provide structured opportunities for CSIRT members to learn about the expertise, experiences, and functional backgrounds of other members

★ Strategy 2: Establish clear individual, team, and MTS goals, roles, and performance standards

Strategy 3: Establish norms for communication transparency in teams and MTSs

★ Strategy 4: Utilize managerial actions that create a psychologically safe climate in the team and MTS

★ Strategy 5: Create opportunities for building strong social connections among CSIRT members to support conflict management

Strategy 6: Increase external connections and social networking to facilitate inter-team and inter-organization trust

SUSTAINED ATTENTION AND FOCUS OVER TIME DURING INCIDENT RESPONSE (CHAPTER 10)

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. My employees pick up on critical incidents toward the ends of their shifts.
2. My employees sustain their attention over the course of their shifts.
3. My employees express satisfaction with the current scheduling of shifts and the length of shifts.
4. My employees claim that shift scheduling leads to improvement in sustaining attention during their shifts.
5. My employees appear to be alert at the end of their shifts.
6. My employees remain focused when dealing with incidents that require overtime work or an extra shift.
7. My employees take the correct amount of breaks during their shifts.
8. After-action reviews have revealed success attributable to sustained attention on the part of an analyst.

IMPROVEMENT STRATEGIES

Strategy 1: Hire job applicants who display a capacity for sustained attention.
- Working memory task
- Brief vigilance (i.e., sustained attention) tasks

★ Strategy 2: Encourage employees to incorporate rest breaks into their shifts.
- Restorative settings
- Socialization

★ Strategy 3: Shift Design – Create a shift plan that reduces sleep disturbances and maximizes attentiveness.
- Work Shift Characteristics
  - Shift length (8-hour shifts recommended)
  - Shift rotation speed (Rapid shift rotations preferred)
  - Shift rotation direction (Forward shift rotation preferred)

CONTINUOUS LEARNING IN INCIDENT RESPONSE (CHAPTER 11)

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. Team members keep up-to-date with developments in cybersecurity.

2. The design of cybersecurity personnels' work roles allows them to develop new skills.

3. Team members engage others outside of my organization to gain new knowledge and skills.

4. Team members maintain contacts with other cybersecurity professionals in order to learn new knowledge and skills.

5. Team members have the opportunity to try out new ideas and processes.

6. Teams discuss how they should interact differently as a result of previous incidents (e.g., in after-action reviews).

7. Thinking about "lessons learned" regarding team interactions or after-action reviews occur in a timely manner after events.

8. Multiple teams working together have the opportunity to try new ideas or processes.

9. Teams participate in activities where they can make errors and learn from their mistakes without these errors being detrimental to the CSIRT performance (e.g., during training sessions).

10. Multiteam information databases (e.g., a Wiki, information board) are used in events.

11. Multiteam information databases (e.g., a Wiki, information board) are used in training.

IMPROVEMENT STRATEGIES

Strategy 1: Select individuals who are creative and curious

Strategy 2: Engage employees' creativity and curiosity as a leader

Strategy 3: Facilitate reflection in teams (team reflexivity or team reflections and adaptation)

★ Strategy 4: Provide feedback in debriefings (After-action Reviews)

Strategy 5: As a leader, promote psychological safety

★ Strategy 6: Improve work design (e.g., feedback, autonomy) to enhance learning

Strategy 7: Create databases to store knowledge

Strategy 8: Use mentoring programs

Strategy 9: Train employees to build networking skills

Strategy 10: Train CSIRT professionals on how to establish a professional, developmental network

★ Strategy 11: Use guided discovery learning

★ Strategy 12: Use error management training

Preface

Preface

To perform at the highest levels, cybersecurity teams must rely on more than technological resources and skills; they also must rely on one of their greatest assets – the collaborative nature of incident responders who work *together* to protect technologies and data from harm. Cybersecurity is not solely technological work; it is collective knowledge work. Leaders and managers of cybersecurity incident response teams (CSIRTs) must be equipped to manage these social dynamics in order to remain effective.

This Handbook highlights social processes and dynamics that contribute to successful collaboration within and between CSIRTs. It also serves to prepare managers to facilitate and maintain the social aspects of cybersecurity through hiring, training and development. We developed this Handbook as part of a three-year research project funded by the Science and Technology Directorate of the U.S. Department of Homeland Security, the National Cyber Security Center in the Netherlands (NCSC-NL), and the Swedish Civil Contingencies Agency (MSB). These sponsors saw a unique opportunity to enhance the development of social dynamics in incident response to allow for greater collaboration not only across individuals and teams, but organizations, broader agencies, and governmental boundaries as well.

The unique quality of this Handbook lies in the fact that we bring scientifically grounded approaches from organizational science to understanding CSIRT collaboration processes and offer empirically-determined strategies to improve these processes. We interviewed cybersecurity professionals across a variety of domains, responsibilities, and countries to identify key factors related to effective collaboration and connected them with proven strategies in the organizational sciences that influence team success. The result is a Handbook that is practical in use, but heavily grounded in science. The strategies provided vary in their relevance and application due to differences among CSIRTs. Where possible, we provide cost and benefit insights about our recommendations to help managers decide which strategies might be most effective for their teams (based on available resources).

Scope of the Handbook

Many manuals, handbooks, and other developmental materials serve as performance aids for cybersecurity professionals but focus solely on individuals' technological skills and/or tools used in incident response. Effective cybersecurity also relies on the collective abilities of cybersecurity professionals to work together. The purpose of this Handbook is to guide CSIRT managers in the development of social processes and factors that drive *team* and *multiteam* performance. We also address individual characteristics (e.g., various knowledge, skills, abilities, and other attributes [KSAOs] such as vigilance) that contribute to individual performance among cybersecurity professionals. We extend our approach beyond individual and team aspects to describe social dynamics and performance management of CSIRT multiteam systems (MTSs) - networks of teams that work closely together to handle complex incidents. Throughout this Handbook, we use the term incident response as a general reference to all performance tasks that occur within or between CSIRTs (recognizing that it can also refer to a particular job function). Further, we use the term "CSIRT" to refer to a variety of teams involved in cybersecurity, although other acronyms are also common (e.g., Computer Emergency Readiness Team - CERT, Security Operation Center - SOC).

Intended Audience

Our intended audience includes primarily managers, team leaders, and Human Resources (HR) staff. Because of the research foundation used in the development of this Handbook, we also expect that applied researchers interested in cybersecurity might read this content. Thus, this Handbook serves two purposes. First, this Handbook can help incident response managers, team leaders, and HR professionals improve hiring decisions, training programs, and their abilities to design and develop effective CSIRTs. Second, this Handbook can guide future programs that aim to improve social dynamics among team members and increase CSIRT effectiveness.

Handbook Structure

This Handbook includes eleven chapters that address various themes identified from our research program. The introductory chapter highlights the importance of social dynamics for incident response and summarizes these themes. This chapter also describes the methods used in our research.

Topics related to the collaborative nature of incident response work and the environment in which such work occurs are covered in early Handbook chapters. Chapter 2 ("The Social Maturity of CSIRTs and Multiteam Systems") provides an overview of the collective nature of cybersecurity work with a focus on CSIRTs as MTSs. Managers can then map out their own CSIRT as an MTS to focus on teams that work closely together.

In Chapter 3 ("Measuring and Evaluating CSIRT Performance"), we address how cybersecurity performance is measured and evaluated, issues with current approaches to performance measurement, and strategies for designing a comprehensive performance measurement program for the entire CSIRT. In Chapter 4 ("Decision-making in CSIRTs"), we address how cybersecurity professionals make critical decisions, challenges faced when making critical decisions, and strategies to improve decision-making.

In the following chapters, we elaborate on individual and social drivers of effective incident response. We begin with Chapter 5 ("Communication Effectiveness in Incident Response",) which describes how to develop communication skills among team members and enhance team and MTS communication. To expand upon Chapter 5, we provide insights into how communication strategies enhance information sharing within and between teams of cybersecurity professionals (Chapter 6, "Information Sharing in Incident Response"). Enhancing collaborative problem solving among individuals and teams in incident response is addressed in Chapter 7 ("Collaborative Problem Solving in Incident Response").

Subsequent Handbook chapters cover topics related to persistent excellence during incident response. Chapter 8 ("Shared Knowledge of Unique Expertise") describes how individuals and teams can build shared knowledge of unique expertise, which helps CSIRT members identify which persons to call on for particular advice on how to address different kinds of incidents. Trust and psychological safety serve as the primary foundation upon which many individual, team, and MTS interactions occur. Methods for building trust among CSIRT and MTS members (including those from other CSIRTs and agencies), as well as developing an environment of psychological safety are reviewed in Chapter 9 ("Trust in Teams and Incident Response Multiteam Systems"). How individuals and teams can sustain

TABLE P.1 SAMPLE CYBERSECURITY SCENARIOS AND AREAS FOR IMPROVEMENT

CYBERSECURITY EXAMPLE	AREAS FOR IMPROVEMENT (RELEVANT HANDBOOK CHAPTER/SECTION)
Many incidents require collaboration across organizational boundaries. However, information varies according to what data is collected, how, and with whom it is shared.	• Communication across teams, organizations, and culture (5) • Identify what information to share, with whom, and how (6, 11) • Identify performance metrics to evaluate whether CSIRTs successfully collaborate, communicate, and share information (3) • Encourage the development of effective networks and networking skills (11) • Enable CSIRTs to function as a multiteam system (2)
Turnover among CSIRT members can be high due to factors such as lack of preparedness or training, burnout from being overworked, person-job fit, among others.	• Develop positive individual and team reactions to stress to enhance resilience (Appendix I) • Promote **a climate of trust and respect among team members (11)** • Increase **individuals' ability to sustain attention and focus over long periods of time (9)** • Identify **appropriate knowledge, skills, abilities, and other characteristics of the job that can be used to select job candidates who "fit" the job (2,5,7)** • Identify **performance gaps that would benefit from training (3)**
Policy requirements place restrictions on what and how information can be shared.	• Understand methods of effective communication (5) and their impact on information sharing (6) • Collaborate to solve problems (7) across team or organizational boundaries (2) • Manage conflict based on disagreements about processes (8)
CSIRT members perform at different levels of ability, sometimes due to differences in experience despite similar training..	• Develop a focus on learning among individuals and within the team, MTS, or organization (11)
Difficulty in distinguishing novel incidents from frequent events makes it hard to predict how an incident should be handled.	• Collaborate to solve problems (7) • Increase individual and team capacity to adapt to novel circumstances (10) • Enable CSIRTs to function as a multiteam system (2)
Unusual events require decision-making about whether to collaborate with others to escalate the event to an incident.	• Identify event and incident characteristics that influence decision-making (4) • Collaborate to solve problems (7) • Communicate with others under stressful circumstances (5) • Identify information to share during incident response (6) • Increase interactions with other teams and/or organizations (2)
Workers complete 12-hour shifts on a regular basis and frequently become stressed and irritable during incidents that require more attention over several days or weeks.	• Maintain **sustained attention and focus over time (10)** • Share **incident information through effective communication during shift changes (5, 6)** • Preserve **individual and team resilience over long periods of time (Appendix I)** • Manage **conflict that results from work pressure or process disagreements (9)**
Analysts tend not to want to request help from other analysts with particular expertise and experiences to collaborate on the resolution of unique incidents.	• Include a focus on an individual's preference for group work in the process for hiring analysts (2) (7) • Develop protocols to determine when analysts should seek help from others (4) • Use training strategies to improve collaboration (7) • Use strategies for developing shared awareness of unique expertise in your team (8) • Use strategies to build trust and psychological safety in your teams (9)
Attempts to collaborate with other analysts or teams with different points of view often result in disruptive conflict.	• Use strategies to build trust and psychological safety in your teams (9) • Employ conflict management strategies to promote constructive exchange of different ideas (9)
Analysts seem unsure about how to respond to unusual events. Delayed responding causes incidents to escalate in severity.	• Develop protocols to determine when analysts should seek help from others (4) • Facilitate use of adaptive case management to facilitate analysts' decision making processes (4) • Use pre-briefing to develop an understanding among team members about how to respond to unusual events (7) • Use strategies to develop and facilitate adaptive thinking (7)

attention and focus throughout lengthy periods of incident management is covered in Chapter 10 (“Sustained Attention and Focus Over Time During Incident Response”). The Handbook concludes with Chapter 11 (“Continuous Learning in Incident Response”), which contains information on how to establish and support a learning climate that encourages CSIRTs and their members to continually adapt to changing conditions.

In the Handbook chapters, we include information on individual knowledge, skills, abilities, and other characteristics (KSAOs) necessary for effective cybersecurity incident response. These KSAOs include technical skills, cognitive abilities, social skills, and other personal attributes necessary to engage individuals in effective and collaborative incident response. Managers can use these KSAO’s to help determine the areas in which their CSIRT is strong or lacking, which can aid hiring decisions.

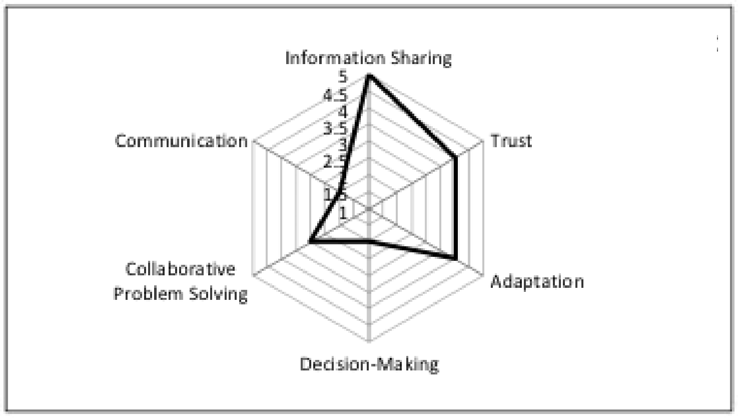
For each chapter, we provide “key themes” to highlight the main points. We begin each chapter with a brief introduction to the topic, followed by Assessment Exercises that can help readers decide if the topic may be an area for improvement in their respective CSIRTs. Prior to describing several recommendations for each topic, we provide background knowledge (e.g., definitions) and information from both the cybersecurity and organizational psychology domains for those readers who are more interested in the data and results from our research. Evidence-based strategies are then provided to guide CSIRT managers on the use of various tools and training to develop and improve the social interactions of their team members. On occasions where our recommendations have yet to be rigorously tested, we provide guidelines for how to determine their effectiveness and relevance (Appendix C: "Hiring and Training CSIRT Employees: Validation Considerations"). We do not recommend implementing such strategies until their effectiveness is determined. This Handbook includes several appendices that support information addressed throughout the chapters (e.g., how to validate selection tools, topical white papers, a CSIRT performance taxonomy).

How to Use this Handbook

Readers can use this book in multiple ways to improve team social dynamics. Ideally, effective social dynamics develop during team (or MTS) formation, although they can develop among fully formed teams. Information from this Handbook can be used to increase situational awareness about social dynamics that influence individual, team, MTS, and organizational performance, or to document team and MTS functions through the use of assessment exercises. We use radar diagrams based on the assessment exercises for CSIRT managers to identify target areas of improvement for their CSIRTs. This method is applied to CSIRT social maturity at the team and MTS levels in Chapter 2 and a blank template can be found in Appendix E. CSIRT managers can use the assessment exercises for each topic to calculate an overall score for that area. Highly effective CSIRTs will have an average score of “5” in each topic area. Lower scores indicate the potential need for improvement in certain areas.

Managers often ask which attribute is most important when hiring new team members. This Handbook helps answer that question by offering managers a diagnostic tool to help determine what attributes they need most in their CSIRT. The assessment exercises in Appendix E allow managers to pinpoint areas in which their CSIRT can benefit from improvement. Once these areas are identified, managers can use the chapters devoted to those topics find KSAO’s that distinguish strong job candidates. We offer some examples of tools that can be used to assess candidates’ skills in particular areas during the interview process (Chapter 5: "Communication Effectivness in Incident Response" and Chapter 2: "The Social Maturity of CSIRTs and Multiteam Systems") and also offer guidelines for how to validate a selection tool for the any of the KSAO’s we identified (Appendix C, “Hiring and Training CSIRT Employees: Validation Considerations”). We note that any measure used in the hiring process should be deemed valid before it is put into practice. If managers decide that hiring is not an option, the recommendations in each chapter can be utilized to improve the skills of individual cybersecurity professionals and team or MTS attributes.

Figure P.1: CSIRT Assessment Example



Handbook information can be tailored to specific incidents or problems faced by cybersecurity professionals as identified by assessment exercises or CSIRT managers. Many CSIRTs face consistent problems, although how they manage those problems likely varies across circumstances. Throughout our research, we identified common CSIRT scenarios, many of which other types of teams also experience, and provide recommendations to improve CSIRT effectiveness in these scenarios. Table P.1 summarizes some of these scenarios and potential areas of improvement.

CSIRT managers can apply radar diagrams to illustrate the results of these assessments. The shape of the diagram is dependent upon the number of topic areas assessed. Using an example from Table P.1, a CSIRT manager could notice that unusual events require team members to make decisions about whether to collaborate with others and to escalate the event to an incident. Assessment exercises related to this example include those from chapters 4 (decision-making), 5 (communication), 6 (information sharing), and 7 (collaborative problem solving). The radar diagram for a team facing this issue might look like Figure P.1. In this particular case, the manager can see that the team could benefit from: 1) development of communication protocols, 2) improvement in team collaboration and 3) enhanced decision-making skills.

Another way to use this book is to think about specific issues that arise with certain types of incidents and focus on those key areas. CSIRT managers or team leaders also could benefit from reading all Handbook sections to familiarize themselves with the social dynamics that influence individual, team, and MTS performance as well as enhance their own knowledge and abilities in an effort to provide better leadership.

Managers can also use several of these tools to take a more proactive approach that establishes an early foundation for CSIRT social maturity. In Table P.2, we describe such an approach, and note which parts of the Handbook can inform each step in a proactive management strategy.

Finally, we provide in Table P.3 several types of recommendations for managers. For instance, some managers may wish to improve the way in which they hire analysts, while other managers may wish to improve the way they train multiteam systems, and yet others may wish to provide decision aids for their analysts. The chapters and appendices in this Handbook focus on a variety of topics, which are conducive to different types of recommendations.. Table P.3 describes the types of recommendations provided in each chapter and appendix in the Handbook.

In conclusion, this Handbook can guide the development of effective social processes involved in cybersecurity incident response. We encourage CSIRT managers to consider these topics and incorporate them into their teams' incident response work to the highest extent possible.

TABLE P.2 USING THE HANDBOOK TO DEVELOP A PROACTIVE MANAGEMENT STRATEGY FOR BUILDING EFFECTIVE CSIRTS

A PROACTIVE MANAGEMENT STRATEGY FOR BUILDING EFFECTIVE CSIRTS	
Develop a job description that includes the social requirements of all CSIRT positions:	• The taxonomy located in Appendix A provides an elaborated classification of performance requirements at individual, team, and multiteam elements. • These requirements should be included in job descriptions that may be used to guide recruitment of position applicants.
Develop clear performance expectations and criteria for future CSIRTs	• Develop a comprehensive performance model to set performance expectations for the team, and provide the basis for future performance evaluations. • Use the information in Chapter 3 for reference
Develop position recruitment materials that specify technical and nontechnical knowledge, skills, and abilities, including cognitive, social, and character attributes	• Chapter 1 in the handbook provides a comparison of KSAOs that are have been listed in current CSIRT job ads, with those defined as key in our research. Appendix G provides an elaborate summary of our research findings. • Throughout the handbook, we reference particular important individual differences. Managers should use this information to identify key requisite KSAOs when preparing recruitment materials.
Develop selection procedures and interview protocols that target nontechnical KSAOs	• See situation interview examples. • Also consider a group staffing focus. See Appendix C on validating such protocols.
Provide entry training and socialization:	• For individuals coming into existing teams, using job shadowing and mentoring programs: See Chapter 8. • For startup teams, managers need to using team charters and other norming protocols to establish communication and information sharing expectations (Chapters 5 and 6). • Managers should also use training simulations to develop shared interaction mental models (see Chapter 7). • For both new individuals and teams, managers should provide clear performance expectations, using balanced scorecard templates. (see an example in Chapter 3.)
Establish protocols and framework for MTS expectations:	• See MTS mapping tool in Chapter 2 and chartering protocols in chapters 5 and 6.
Sustain operational effectiveness by creating a continuous learning climate:	• See Chapter 11.

TABLE P.3 RECOMMENDATIONS BY CHAPTER

CHAPTER OR APPENDIX IN HANDBOOK	EMPLOYEE SELECTION (HIRING)	INDIVIDUAL ANALYST TRAINING	TEAM AND MULTITEAM SYSTEM TRAINING	PERFORMANCE ASSESSMENT AND MGMT	PROCESS MGMT	BOUNDARY MGMT	DECISION AIDS	WORK AND ORGANIZATIONAL DESIGN
Exective Summary (Quick Reference Guide)								
Introduction to the Handbook								
The Social Maturity of CSIRTs and Multiteam Systems	X			X	X	X		
Measuring and Evaluating CSIRT Performance				X			X	
Decision-Making in CSIRTs	X	X	X		X		X	
Communication Effectiveness in Incident Response	X		X			X	X	X
Information Sharing Effectiveness in Incident Response					X			
Collaborative Problem-Solving in Incident Response	X		X		X			
Shared Knowledge of Unique Expertise		X	X		X			
Trust in Teams and Incident Response Multiteam Systems		X			X			
Sustained Attention and Focus Over Time During Incident Response	X	X						X
Continuous Learning in Incident Response	X	X	X					X
CSIRT Performance Taxonomy				X				
Assessment Exercises and Improvement Strategies				X				
Hiring and Training CSIRT Employees	X	X	X					
Training Programs of Instruction		X	X					

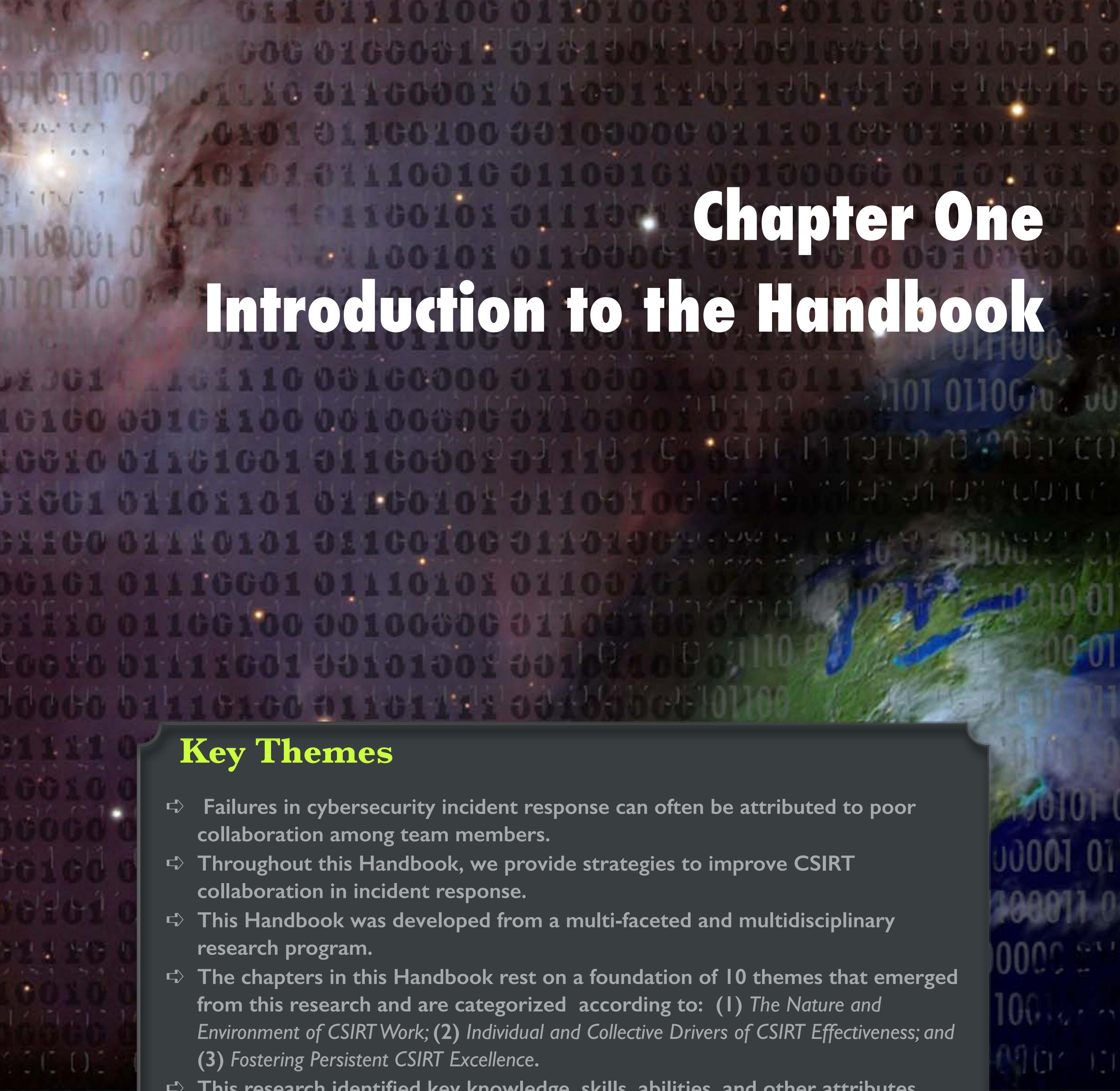
Note: "X" in a cell indicates that a particular handbook chapter or appendix possesses recommendations in a particular area.

TABLE P.3 RECOMMENDATIONS BY CHAPTER (CONTINUED)

CHAPTER OR APPENDIX IN HANDBOOK	EMPLOYEE SELECTION (HIRING)	INDIVIDUAL ANALYST TRAINING	TEAM AND MULTITEAM SYSTEM TRAINING	PERFORMANCE ASSESSMENT AND MGMT	PROCESS MGMT	BOUNDARY MGMT	DECISION AIDS	WORK AND ORGANIZATIONAL DESIGN
Supplemental “Worksheets”					X		X	
Learning from Other Teams			X		X		X	
Comparing Knowledge, Skills and Abilities (KSAs) Necessary for Cybersecurity Workers in Coordinating and non-Coordinating CSIRTs	X							
Building Informal CSIRT Networks						X		
Social Resilience	X	X						

Note: “X” in a cell indicates that a particular handbook chapter or appendix possesses recommendations in a particular area.

Chapters



Chapter One
Introduction to the Handbook

Key Themes

- Failures in cybersecurity incident response can often be attributed to poor collaboration among team members.
- Throughout this Handbook, we provide strategies to improve CSIRT collaboration in incident response.
- This Handbook was developed from a multi-faceted and multidisciplinary research program.
- The chapters in this Handbook rest on a foundation of 10 themes that emerged from this research and are categorized according to: (1) *The Nature and Environment of CSIRT Work;* (2) *Individual and Collective Drivers of CSIRT Effectiveness; and* (3) *Fostering Persistent CSIRT Excellence.*
- This research identified key knowledge, skills, abilities, and other attributes (KSAOs) that contribute to effective cybersecurity incident response.
- This Handbook provides information on these KSAOs, along with recommended strategies for developing them.

Contents

1.0 Introduction to the Handbook

Responding to cybersecurity crises can be an intense *social* process. For all but the most routine incidents, at least two or more analysts typically collaborate in their resolutions. Examples of such CSIRT collaboration include:

- Within a CSIRT
  - A novice analyst seeks help from experienced analysts to determine if and how an event poses a threat and whether it should be escalated.
  - Forensics analysts work with malware analysts to uncover incident root causes.
- Between teams within an organization
  - A CSIRT manager works with the organization's legal team and top management team executives to determine organization liability or risk related to mitigation strategies.
- Between different organizations
  - A corporate CSIRT is required to work with law enforcement and other government agencies when an incident involves the loss of intellectual property or other forms of theft.
  - A national CSIRT collaborates with CSIRTs from other countries to handle incidents or take proactive measures to mitigate threats.

Our research, to be described later, demonstrates that factors such as the novelty of detected cyber incidents, high political visibility, or the impact of particular threats will lead to increasingly intense interactions and coordination among many analysts and incident response groups. The above examples indicate that whereas cyber infrastructure and software technology are critical components of cyber defense, so are social processes among incident responders and other cybersecurity professionals. Effective incident response entails an effective integration of *both* technological and social processes.

1.0.1 TEAM COLLABORATION FAILURES

Studies of cybersecurity incident response failures often focus on technological breakdowns as central causes (e.g. Abrams & Weiss, 2008; Grimaila, Schechtman, Mills & Fortson, 2009). However, as with other types of teams, failure also can result from poor coordination and collaboration – in other words, breakdowns in social processes. Such breakdowns are common causes of failure in all types of teams. Indeed, organizational scientists have noted, "failures of team leadership, coordination, and communication are well documented causes of the majority of air crashes, medical errors, and industrial disasters" (Kozlowski & Ilgen, 2006, p. 78). Some examples of such failures in non-cyber settings include:

- *Medicine:* 98,000 deaths in the U.S. each year are caused by medical errors (Kohn, Corrigan, & Donaldson, 1999), 70% of which are linked to systemic failures in teamwork, communication, and coordination (Studdert, Brennan, & Thomas, 2002).
- *Weather Response:* The effects of Hurricane Katrina, one of the deadliest hurricanes in the history of the U.S., were exacerbated by coordination and communication failures at multiple levels of the U.S. government (U.S. Executive Office of the President, U.S. Assistant to the President for Homeland Security and Counterterrorism, 2006; U.S Department of Defense, National Guard, 2005; U.S. Department of Homeland Security, Federal Emergency Management Agency, 2005).
- *Terrorist Attacks:* Responses to the September 11, 2001, attack on the Twin Towers in the U.S. were hampered by numerous communication failures at the federal government level (9/11 Commission staff statement No.17, 2001), as well as among different first responder groups (Dwyer, Flynn, & Fessenden, 2002). "Throughout the crisis, the two largest emergency departments, Police and Fire, barely spoke to coordinate strategy or to share intelligence about building conditions" (Dwyer, Flynn, & Fessenden, 2002, para. 10).
- *Oil Spills:* The BP Oil spill in the Gulf of Mexico was triggered in part by failures in communication and coordination among groups associated with BP, who operated the Deepwater Horizon rig, and Transocean, which leased the rig to BP (De Wolf & Mejri, 2013). The White House oil spill commission attributed the blame to the associated companies for failing to share important information (Goldenberg, 2010).
- *Airplane disasters:* Reports have documented that 70-80% of aviation accidents of the U.S. national airspace are due to pilot-related factors (Shappell & Wiegmann, 1996); communication failures are often the most prominent of such factors (Illman & Gailey, 2012).

Similar examples come from the context of cybersecurity incident response:

- *Sony (2014):* Reports noted that "lack of information and consultation led to flip-flops [and] confusion" (Barrett & Yadron, 2015, subheading). This attack indicated "major shortcomings in how the government and companies work together to respond to attacks" (Barrett & Yadron, 2015, para. 2). "Companies and agencies…hewed so closely to their own interests that some decisions were based on little information or consultation" (Barrett & Yadron, 2015, para. 4).
- *DigiNotar (2011):* After detecting a break-in on their systems, DigiNotar personnel "decided to keep it a secret from the general public and the authorities," delaying response and damage control among multiple stakeholders (Ministry of Security and Justice, the Netherlands; Federal Office for Information Security, Germany; Swedish Civil Contingencies Agency, Sweden, 2014; p. 8).
- *Deutsche Telekom AG (2012):* Responses were delayed to

stop an attack partly because of ambiguity in responsibilities for responding to the attack. Accordingly, the Federal Criminal Police Office only acted after Telekom provided additional clarifying information (Ministry of Security and Justice, the Netherlands; Federal Office for Information Security, Germany; Swedish Civil Contingencies Agency, Sweden, 2014).

- *Tieto (2011)*: To mitigate the effects of a hardware error at Tieto, an IT service provider, the Swedish Civil Contingencies Agency (MSB) requested situation reports from Tieto and the affected organizations. Initial information sharing was hampered due to concerns about commercial confidentiality. Moreover, an analysis of this event found that "several of the affected parties did not have enough knowledge about their own dependencies, nor about their need for cooperation." (Ministry of Security and Justice, the Netherlands; Federal Office for Information Security, Germany; Swedish Civil Contingencies Agency, Sweden, 2014; p. 23; The Swedish Civil Contingencies Agency, 2012).

1.0.2 THE IMPORTANCE OF SOCIAL PROCESSES TO CYBERSECURITY INCIDENT RESPONSE

These examples of collaboration failure in both non-cyber and cybersecurity teams point to the criticality of social processes for high performance during incident response. In our research with

TABLE 1.1 COLLABORATION CHILLERS IN CSIRTs: QUOTES FROM THE FIELD

Failure to share unique information	• "What I had last year was a team of people who weren't really doing the open communication at the level I wanted. So that's a problem in the team."
Failure to initiate necessary collaboration	• "We also see that it is a cultural thing probably and some of our entities have incidents and they do not contact us. So the incident inside the country escalates, and if they would have asked us, we would have helped them in an instant and it would not be as big as it turned out to be."
Failure to adapt	• "We have to be able to be as flexible as the attack and we have to be able to stay at the bleeding edge of current methods of detecting these attacks and handling these intrusions. If we can't do that, then we're dead in the water. The attackers are extremely agile and we have to be as well."
Poor communication practices	• "The communication is lacking. We don't interact as well as maybe we could've. We're not a finely gelled team."
Poor listening	• "…You either have to just get somebody else to come in and tell them what's going on, or go to the boss and say they're screwing this thing up. I tried to help them, it's just they're not listening."
Lack of trust	• "I would say nine times out of ten, I handle it myself. I don't rely on the other two for having any clue as to what they're doing."
Lack of knowledge about team member expertise	• "A lot of times, it's lack of awareness. They don't know I'm here."
Interpersonal conflict	• "My forensics guys are completely different than my incident handlers because they require different things… So they never get along… when I first had them in the lab, my incident response guys literally walled themselves away from the forensics team…they didn't want to associate with each other."

cybersecurity professionals, we interviewed many individuals and team leaders who spoke about the importance of communication, collaboration, and coordination for the effectiveness of their teams. They also pointed to failures in these processes as critical issues for team effectiveness. Quotes from these interviews, shown in Table 1.1, identify several *collaboration chillers* that occur in many CSIRTs, including:

- Failure to share unique information
- Failure to initiate necessary collaboration
- Failure to adapt
- Poor communication practices
- Poor listening
- Lack of trust
- Lack of knowledge about team member expertise
- Interpersonal conflict

We will describe these potential problems in this Handbook, as well as provide recommendations for managers to fix them.

The main theme of our work is that the effectiveness of cybersecurity incident response rests on both *technological* and *social* capacities--*both are necessary; neither alone is sufficient.* Yet, despite the joint importance of these capacities, most manuals and handbooks designed to increase CSIRT effectiveness focus mainly on technology-related processes. These documents typically cover topics such as:

- CSIRT frameworks, services, and functions (Bowen, Hash, & Wilson, 2006; West-Brown et al., 2003);
- Information security governance (Bowen et al., 2006);
- Information security tools and information assurance techniques (Harvey, 2012; West-Brown et al., 2003);
- Information sharing between organizations (NICE, 2014); and
- Technical skills for incident responders (Harvey, 2012; West-Brown et al., 2003).

When documents do address team aspects of cybersecurity incident response, the emphasis is typically on individual functions and roles within the CSIRT and incident response process flow. What existing cybersecurity manuals do not cover in sufficient detail are the social processes and dynamics that contribute to effective incident response. ***Improving social processes and dynamics is the purpose of this Handbook.***

1.1 Research Foundation for the Handbook

This Handbook was developed as the culmination of a research effort jointly funded by the U.S. Department of Homeland Security (DHS), the National Cyber Security Centre (NCSC) of the Netherlands, and the Swedish Civil Contingencies Agency (MSB). This effort joined scientists from three institutions, George Mason University, Dartmouth College, and Hewlett- Packard, to create a large multidisciplinary research team. In the following sections we describe (a) the research activities that contributed to the content of this Handbook, and (b) the major research themes uncovered by these activities.

Research Activities that Contributed to this Handbook

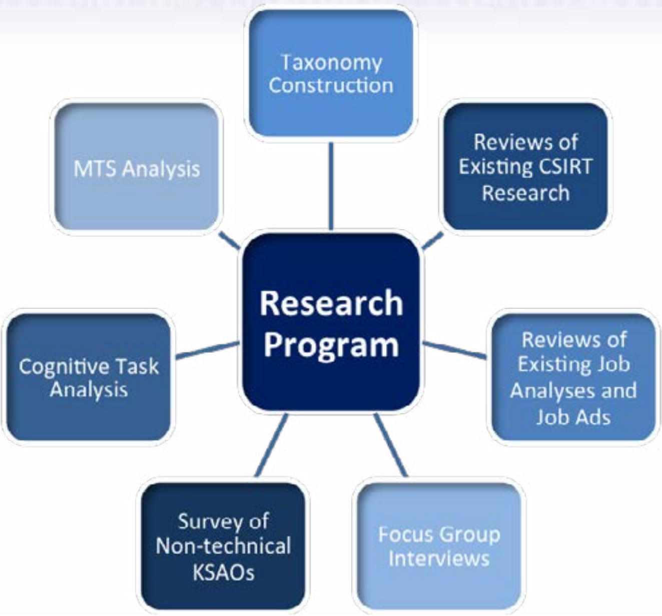

Research Program
Taxonomy Construction
Reviews of Existing CSIRT Research
Reviews of Existing Job Analyses and Job Ads
Focus Group Interviews
Survey of Non-technical KSAOs
Cognitive Task Analysis
MTS Analysis

Figure 1.1 Projects Comprising the CSIRT Effectiveness Research Program

One purpose of our research effort was to examine CSIRT MTSs (described below and covered in detail in Chapter 2 ("The Social Maturity of CSIRTs and Multiteam Systems") that are typically used to resolve cybersecurity incidents. Another purpose was to define the planning processes, behaviors, and outcomes that reflect successful CSIRT performance at the individual, team, and MTS level. These elements of performance were used to identify the individual knowledge, skills, abilities and other characteristics (KSAOs), the team and MTS attributes, and work design characteristics that are important for effective CSIRT performance. This information served as one basis for our recommendations for performance improvement.

Several different projects comprised the research effort that contributed to this Handbook (see Figure 1.1; also Chen et al., 2014). These projects included the following:

- *Construction and Validation of an Incident Response Performance Taxonomy:* Our research team developed a taxonomy of cybersecurity incident response performance based on reviews of general team performance and specific CSIRT literatures. This taxonomy (presented in Appendix A) indicates three dimensions of cybersecurity performance: **level** (individual, team, and multiteam

[1] For more information on the development and analysis of this CSIRT taxonomy, please see Zaccaro et al. (2016).

systems), **timing** (proactive versus reactive processes), and **phase** (planning versus execution activities) [1]. Data from focus groups (see below) were used to provide an initial validation of the taxonomy. We used this taxonomy to derive KSAOs necessary for effective cybersecurity performance. Managers also can use the elements in this taxonomy to develop fine-tuned performance appraisal tools, selection tools, and training programs to develop individual and collective incident response skills (see Appendix A for more details).

- *Reviews of Existing CSIRT Research:* A starting point for our research effort was a comprehensive review of existing academic and applied research on CSIRT effectiveness. Our intent was to ensure that our own effort began from current knowledge about CSIRTs, and to provide a basis for added value to this literature. This review contributed, in part, to the construction of the taxonomy of cybersecurity incident response performance.
- *Review of Existing CSIRT Job Analyses:* One tool of organizational psychologists is the job analysis, which is used to determine the key elements of work in particular positions (Cascio & Aguinis, 2010). Another aspect of the job analysis is the identification of social requirements for such work (Fleishman & Quaintance, 1984). Several analyses have been completed regarding the technological requirements of incident response work (e.g. NICE, 2013; West-Brown et al., 2003; Wolf, 2004). We did not replicate this work; instead we used it to validate parts of our taxonomy and derive technical knowledge and skills necessary for CSIRT performance. The main focus in our job analysis of incident response in this study was on the cognitive, social, personality, and motivational requirements of such work.
- *Review of Job Ads for CSIRT Positions:* Another task in our effort was the review of 111 job advertisements for cybersecurity personnel hires. Our purposes were to (a) identify the KSAOs typically sought by cybersecurity managers, and (b) identify gaps between such KSAOs and those attributes identified as important in our research. The results of this review are located in several places throughout the Handbook.
- *Focus Group and Managerial Interviews:* To our knowledge, our research involved one of the most comprehensive sets of interviews of incident responders in a single study. We conducted 52 focus group interviews with a total of approximately 150 participants. We interviewed 28 MTS representatives from organizations across the United States, the United Kingdom, Germany, Sweden, and the Netherlands (See Chapter 2 "The Social Maturity of CSIRTs and Multiteam Systems"). The types of CSIRTs represented in our study included national, government, and military coordinating CSIRTs, managed security service providers (i.e., external clients), Corporate CSIRTs and academic institution CSIRTs. The data from these interviews were used to:
  - Develop a core set of propositions about the social dynamics of cybersecurity incident response work;
  - Validate the incident response performance taxonomy;
  - Derive an initial set of incident response KSAOs;
  - Provide qualitative data for use in this Handbook and in CSIRT training exercises.
- *Survey of Non-Technical Knowledge, Skills, Abilities, and other Attributes:* Prior studies of CSIRTs delineated technical KSAOs necessary for successful incident response (NICE, 2013). These studies generally did not examine cognitive, social, and character attributes that also influence CSIRT performance. Accordingly, as part of this effort, we developed a comprehensive list of such attributes from our taxonomy, focus group interviews, and from a survey of 88 CSIRT professionals. The results of this survey are described throughout the Handbook and are summarized in Appendix G.
- *Cognitive Task Analysis:* Most job analyses focus on the behaviors required for job performance. However, because our taxonomy indicated the centrality of knowledge work in incident response, we also conducted a cognitive task analysis (CTA) designed to identify the particular cognitive skills that contribute to effective CSIRT performance. The results of this analysis are described throughout the Handbook, and are summarized in Chapter 4 ("Decision-making in CSIRTs").
- *MTS Analysis:* As noted above, one of the primary contributions of our research (and this Handbook) was to examine CSIRTs as MTSs. Different processes and dynamics are relevant for MTSs that are not equally relevant for traditional teams. An MTS does not refer simply to the collection of teams working in a CSIRT, but highlights the fact that multiple teams collaborate closely to solve complex problems. This concept was introduced to organizational science in 2001 (Mathieu, Marks, & Zaccaro, 2001) and applied in many organizational settings, including military, health, transportation, business, and disaster recovery settings (e.g. DeChurch & Marks, 2006; DeChurch et al., 2011; Goodwin, Essens, & Smith, 2012; Zaccaro, Marks, & DeChurch, 2012). We have applied the MTS concept here to the domain of cybersecurity incident response (see also Chen, et al., 2014). As part of this effort, we analyzed the composition and interaction patterns of 28 incident response MTSs. The results of this analysis are described in Chapter 2 ("The Social Maturity of CSIRTs and Multiteam Systems"), along with practical tools for CSIRT managers.

1.2 Major Research Themes and Findings

The chapters in this Handbook rest on a foundation of several research themes that emerged from our study. In this section, we briefly summarize 10 themes and point to the specific chapters that elaborate on them. These themes are grouped under three categories: *(1) The Nature and Environment of CSIRT Work; (2) Individual and Collective Drivers of CSIRT Effectiveness; and (3) Fostering Persistent CSIRT Excellence.*

1.2.1 CATEGORY 1: THE NATURE AND ENVIRONMENT OF CSIRT WORK

The first two research themes should be quite obvious and unsurprising to readers of this Handbook. Yet, we note them because they provide an important foundation for the research other themes listed below.

Theme 1: Cybersecurity incident responders perform individual and collective knowledge work.

To understand what individual capacities and team processes drive CSIRT effectiveness, we need to first describe the nature of the work. Organizational scientists have labeled activities similar to cybersecurity incident response as knowledge work. According to these scientists:

> "The main feature differentiating knowledge work from other conventional work is that the basic task of knowledge work is thinking. Although all types of jobs entail a mix of physical, social, and mental work, it is the perennial processing of non-routine problems that require non-linear and creative thinking that characterizes knowledge work" (Reinhardt, Schmidt, Sloep, & Drachsler, 2011, p. 150).

Relevant to this definition, the core performance functions of incident response work entail complex thinking and problem-solving. As cyber events are becoming more complex, collective knowledge work among multiple analysts is becoming more necessary (also see Theme 4). Chapter 4 ("Decision Making in Cybersecurity Incident Response Teams") describes the event and incident characteristics that influence decision processes in such work.

Theme 2: Cybersecurity incident responders often need to work within volatile, uncertain, complex, and ambiguous environments (i.e., "VUCA"; Stiehm, 2002; Scott, 2012).

This research theme describes the environment within which CSIRT knowledge work occurs. Much incident response work is fairly routine. For example, watch team members (i.e., analysts who monitor computers and networks for incidents and flag unusual patterns) often are the first level of incident response, routinely handling many incidents and spending a large proportion of their time attending to uneventful data streams across computer screens. However, the relatively routine nature of such work can switch quickly into a more uncertain and volatile mode when novel and/or potentially high impact cyber threats are detected. Thus, both incident response work and the nature of cyber events themselves can move from routine to novel and very quickly with little warning. The implications for this aspect of CSIRT work include the following:

- The dynamic nature of the incident response work environment requires individual analysts and CSIRTs to be adaptive in how they approach incident problem-solving (also see Theme 9). We cover suggested strategies and approaches for increasing adaptation in Chapters 7 ("Collaborative Problem Solving in Incident Response") and Chapter 11 ("Continuous Learning in Incident Response").
- The elements of volatility, uncertainty, complexity, and ambiguity (VUCA) of the incident response environment contribute to stress felt by analysts. When stress is continuously experienced at high levels, performance can degrade by significant amounts. Accordingly, both individuals and teams need to possess a strong degree of resilience (also see Theme 9). Appendix I in this Handbook provides suggestions on how CSIRT managers can mitigate stress among analysts and foster greater individual and collective resilience in addition to technical and operational resilience.

Theme 3: Maintaining vigilance (i.e., sustained attention and focus over time) is a substantial problem because of the length of shifts and the nature of CSIRT work.

One specific element of cybersecurity work that received extended focus in this research effort was the attentional capacity of cybersecurity professionals and teams. Watch team activities require sustained attention while scanning events for potential threats. Likewise, the shift schedules of most CSIRTs and the high cognitive demands of the work itself can exhaust cognitive capacities needed for acute situational awareness. We noted above that incident response work can move unpredictably from very routine to highly novel situations. The pace of incoming information also can change rapidly. Loss of attentional and cognitive capacity, however, can impair the ability of incident responders to shift their focus when required. Accordingly, the maintenance of vigilance is a particularly critical element of CSIRT performance. Chapter 10 ("Sustained Attention and Focus over Time") in this Handbook provides additional insight on this issue and offers strategies to help CSIRT managers maintain individual and team vigilance.

Theme 4: Cybersecurity incident response occurs at multiple levels, including individual, team, and multiteam systems.

Organizational scientists have argued that work in environments with high levels of VUCA can be too demanding for individual performers, requiring the joint contributions of multiple people (Scott, 2012). In other words, as we noted above, CSIRT work often entails collective knowledge work where multiple analysts need to work together to resolve incidents. Our research confirmed that while individuals working alone complete a significant amount of incident response work, an equal or greater amount of this work is performed by two or more individuals working together. Our research also indicated that a significant amount of incident response work is completed by MTSs, or multiple teams working together.

The strong collaborative nature of incident response work carries several implications for CSIRT managers:

- Communication and information sharing are essential parts of effective performance. Again, this statement is not surprising. However, most descriptions of information sharing in the cybersecurity literature do not make some critical distinctions that are important for CSIRT managers. Chapter 6 ("Information Sharing Effectiveness in Incident Response") describes a framework of incident response information sharing that reflects these distinctions. Chapter 6 also includes implications for CSIRT managers, along with strategies to improve communication (see Chapter 5, "Communication Effectiveness in Incident Response," as well).
- Incident response collaboration takes the form of collective knowledge work. Such "thinking together" means that members of CSIRTs generate ideas together, and then evaluate and revise those ideas together as a group. CSIRT managers must create the best conditions for facilitating this "thinking together" within their teams and MTSs. Chapter 7 ("Collaborative Problem-Solving in Incident Response") provides more information on collaborative problem-solving along with strategies that can be implemented by CSIRT managers and team leads.

Theme 5: Incident response collaboration within and between incident responders and teams is typically discretionary.

One of the key findings of our research is that incident response collaboration is typically a decision or choice made by an individual analyst upon detection and triage of a particular incident. Not all incidents are escalated to include other team members or other teams. Thus, a central process in incident response performance is the choice to work with additional analysts or responders in the resolution of a particular incident. Several parameters determine this choice, including (a) existing policies and guidelines; (b) the nature of the event (e.g., its severity, political impact); (c) characteristics of the team members and other teams to be included in the collaboration (e.g., degree of trust and expertise in the team and MTS); and (d) characteristics of the individual responder (e.g., comfort with or preference for working with others). Chapter 4 ("Decision Making in CSIRTs") covers discretionary collaboration and escalation along with critical incident characteristics that trigger collaboration. Furthermore, Figure 4.1 depicts the myriad discretionary choices during incident response that are encountered by analysts.

Theme 6: What constitutes good performance among cybersecurity incident responders is not well understood. Performance should be evaluated directly using appropriate metrics—not indirectly (e.g., not only using existing maturity models).

A core objective of our research effort was to specify the drivers of effective CSIRT performance at the individual, team, and MTS levels. We found in our interviews that defining the nature and elements of good performance was difficult, and there were not high levels of agreement among interviewees. These insights are in line with those from cybersecurity literature, which reflects a general dissatisfaction with the metrics that are used to evaluate cybersecurity performance (e.g., Rashid, 2015). The lack of well-defined and widely-accepted performance metrics creates barriers to many important managerial responsibilities including: 1) identification of areas of strengths and weaknesses of cybersecurity professionals, teams, and MTSs; 2) effective decision-making regarding resource allocation (e.g., training to address an identified area of weakness); and 3) accurate comparisons of cybersecurity professional, team, and MTS performance that can improve decisions regarding personnel (e.g., promotions). Chapter 3 ("Measuring and Evaluating CSIRT Performance") addresses these issues by providing a discussion of performance metrics and ratings as well as recommendations for evaluating CSIRT performance. These recommendations include assessing of team and MTS performance. In addition, the taxonomy in Appendix A includes a range of performance outcomes relevant for CSIRTs.

Organizational scientists refer to lower performance in teams due to poor collaboration as process loss (Steiner, 1972). In this Handbook, we use the term social maturity to refer to teams and MTSs that have established social processes and team states that promote and sustain high levels of collective performance. Chapter 2 ("The Social Maturity of CSIRTs and Multiteam Systems") describes this concept in more detail.

1.2.2 CATEGORY 2: INDIVIDUAL AND COLLECTIVE DRIVERS OF CSIRT EFFECTIVENESS

Theme 7: Four sets of knowledge, skills, abilities, and other attributes (KSAOs) are necessary for effective cybersecurity incident response work. These include: technical skills, cognitive abilities, social skills, and personal character.

One of the primary purposes of our research was to define the individual and team attributes that drive effective incident response performance. As we have noted, most discussions of CSIRT KSAOs have focused on the technical skills and knowledge necessary for such performance. As stated above in our research activity overview, we used several strategies to specify other possible KSAOs, including the performance taxonomy, team performance literature, focus group interviews, and cognitive task analyses. We then surveyed 88 cybersecurity cyber analysts from either a coordinating or non-coordinating CSIRT, and asked them to rate the importance of each of the non-technical KSAOs. We found that the top 20 KSAOs that were ranked as most important by cybersecurity professionals included specific attributes across all non-technical categories: cognitive abilities, social skills, and personal character (more details of our findings from the KSAO survey are reported in Appendix G). However, a key observation from our work is that job ads for cybersecurity positions rarely focus on the full range of non-technical skills indicated in our findings. Table 1.2 displays a comparison of the skills typically appearing in job ads with those top 20 KSAOs identified through our research. The lack of correspondence between the job ads and critical non-technical KSAOs identified in our research suggests that HR departments associated with CSIRTs and hiring managers need to pay more attention to non-technical KSAOs in their recruitment, assessment, and selection of candidates for cybersecurity positions.

Theme 8: Team- and MTS-level states and protocols also contribute to CSIRT effectiveness.

Individual KSAOs are necessary but not sufficient for effective CSIRT performance. Our focus group interviews and our reviews of team effectiveness research, and particularly reviews of teams similar to CSIRTs (Steinke et al., 2015) indicated that particular shared cognitive and affective states are also important for successful incident response collaboration. These include:

- Trust;
- Shared knowledge of each member's unique expertise and experiences;
- Shared understanding of how team members need to interact when resolving incidents, particularly high threat

TABLE 1.2 COMPARISON OF TOP 20 KSAOs

TOP 20 NON-TECHNICAL KSAOs FROM OUR RESEARCH	KSAOs TYPICALLY APPEARING IN JOB ADS, O*NET, AND NICE
Social/Team	**Social/Team**
• Trustworthiness	• Communication skills
• Collaborative problem-solving	• Leadership / Management skills
• Motivation to work on behalf of team	• Interpersonal skills
• Communication skills	**Cognitive**
• Mentor/coaching ability	• Reasoning skills (Intelligence)
Cognitive	• Decision-making competence
• Learning ability	**Character**
• Problem-solving skills	• Self-motivation
• Investigative skills	**Technical**
• Intelligence	• Vulnerability analysis skills
• Decision-making competence	• Knowledge of legal, government and jurisprudence requirements
Character	• Knowledge of incident management
• Work ethic	• Skills of computer languages
• Specific curiosity	• Knowledge of infrastructure design
• Resilience	• Technology trend awareness
• Self-motivation	• Knowledge of information systems/network security
• Detail-orientation	• Software development and engineering skills
• Proactive	• Intrusion prevention skills
• Adaptive	• Knowledge of network management methods
• Perseverance	• Digital forensics skills
• Diverse curiosity	• Knowledge of organizational processes and operations
• Ambiguity tolerance	• Knowledge of operating systems
	• General IT knowledge

Note: Circled KSAOs indicate correspondence between our research findings and job ads.

incidents (i.e. shared team interaction models);

- Communication and information sharing norms/protocols; and
- Conflict management norms/protocols.

These five characteristics are not only important for collaboration within incident response teams, but also between teams in a CSIRT MTS. Chapters 8 and 9 in the Handbook ("Shared Knowledge of Unique Expertise" and "Trust in Incident Response Teams and Multiteam Systems," respectively) describe in more detail the importance of these team and MTS states for effective CSIRT performance. We provide recommendations to managers and team leads to foster the development of these cognitive and affective states.

1.2.3 CATEGORY 3: FOSTERING PERSISTENT CSIRT EXCELLENCE

The final two research themes that emerged from our work focus on qualities that promote continued or persistent excellence in CSIRTs.

Theme 9: Adaptation and resilience across all levels are vital to effective cybersecurity incident response.

We have noted that the dynamic nature of the CSIRT work environment requires that incident responders be adaptive in terms of how they think about and resolve problems. Cognitive researchers have shown that people tend to think in habitual ways, rarely changing how they frame problems, even when circumstances change substantially (e.g. Duncker & Lees, 1945; Wertheimer, 1954). Other research has also revealed that routines are often disrupted in emergencies, and that emergency response requires adaptive management (Brooks, Bodeau, & Fedorowicz, 2010). Likewise, at the team- and MTS-level the propensity to engage in habitual thinking and actions is made worse by tendencies toward "groupthink" and by conformity pressures that often exist in teams and MTSs (Festinger, 1950; Janis, 1972).

Accordingly, a major element in adaptive thinking is a capacity to engage in "frame switching," or the application of new frames of reference to different kinds of problems (Nelson, Zaccaro, & Herman, 2010). Such capacity is especially important in the dynamic CSIRT environment. However, current CSIRT training approaches do not typically utilize strategies shown to develop adaptive thinking skills, neither among individual analysts or in CSIRTs. Chapters 7 ("Collaborative Problem-Solving in Incident Response") and 11 ("Continuous Learning in Incident Response"), describe factors that drive individual, team, and MTS adaptability, and strategies for managers to promote these factors.

We have noted that the CSIRT work environment contains a range of stressors that increase the challenge confronting incident responders. These stressors can have deleterious effects on individual well-being as well as on the team and MTS's capacity to maintain high collective performance. Thus, CSIRT managers need to utilize strategies designed to increase individual and team resilience in the CSIRT environment. Appendix I presents a number of best practices for managers to promote such resilience.

Theme 10: Effective cybersecurity incident response work requires continuous learning across all levels.

Finally, we noted earlier that the nature of incident response as collective knowledge work requires that incident responders, teams, and MTSs establish a sustained learning climate that encourages them to continually refresh and expand their knowledge and understanding about cybersecurity. In our interviews, we found that managers of more effective CSIRTs tended to provide opportunities for individuals to gain new experiences and to share new knowledge with other team members. Such CSIRTs possessed an environment of experimentation, where errors were viewed as learning opportunities. Mature CSIRTs also use the knowledge and experiences they collect to continually adapt their processes and systems. Chapter 11 ("Continuous Learning in Incident Response") offers information and strategies on how CSIRT managers can create and sustain a learning environment in their teams and MTSs.

1.3 Summary

Responding to cybersecurity crises entails both technological and social processes. Most existing CSIRT manuals emphasize the former. This Handbook focuses on the latter, and particularly on enhancing incident response collaboration within and between cybersecurity teams. The Handbook is based on the results of an extensive research program that identified key KSAOs necessary for performance. Our research also identified multiteam systems as a key organizational form for CSIRTs. In the next chapter, we define this form in more detail, and provide information to managers on leading MTSs.

References

9/11 Commission staff statement No.17. (2001). Improvising a homeland defense. Retrieved from: http://govinfo.library.unt.edu/911/staff_statements/staff_statement_17.pdf

Abrams, M., & Weiss, J. (2008). Malicious control system cyber security attack case study–Maroochy Water Services, Australia. *McLean, VA: The MITRE Corporation.*

Barrett, D., & Yadron, D. (2015, February 22). Sony, U.S. agencies fumbled after cyberattack. Retrieved from http://www.wsj.com/articles/sony-u-s-agencies-fumbled-after-cyberattack-1424641424

Bowen, P., Hash, J., and Wilson, M. (2006). *Information security handbook: A guide for managers* (NIST Special Publication 800-100). National Institute of Standards and Technology: Gaithersburg, MD.

Brooks, J. M., Bodeau, D., & Fedorowicz, J. (2013). Network management in emergency response articulation practices of State-level managers—Interweaving up, down, and sideways. *Administration & Society, 45*(8), 911-948.

Cascio, W. F. and Aguinis, H. (2010). Applied psychology in human resource management (7th Ed). Prentice Hall.

Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Gorab, A. K. (2014). An organizational psychology perspective to examining computer security incident response teams. *IEEE Security & Privacy, (5),* 61-67.

De Wolf, D., & Mejri, M. (2013). Crisis communication failures: The BP case study. *International Journal of Advances in Management and Economics*, *2*(2), 48-56.

DeChurch, L. A., & Marks, M. A. (2006). Leadership in multiteam systems. *Journal of Applied Psychology*, 91(2), 311-329.

DeChurch, L. A., Burke, C. S., Shuffler, M. L., Lyons, R., Doty, D., & Salas, E. (2011). A historiometric analysis of leadership in mission critical multiteam environments. *The Leadership Quarterly*, *22*(1), 152-169.

Duncker, K., & Lees, L. S. (1945). On problem-solving. *Psychological monographs*, *58*, i-113.

Dwyer, J., Flynn, K., & Fessenden, F. (2002, July 6). Fatal confusion: A troubled emergency response; 9/11 exposed deadly flaws in rescue plan. Retrieved from http://www.nytimes.com/2002/07/07/nyregion/fatal-confusion-troubled-emergency-response-9-11-exposed-deadly-flaws-rescue.html

Festinger, L. (1950). Informal social communication. *Psychological Review, 57*, 271-282.

Fleishman, E. A., & Quaintance, M. K. (1984). *Taxonomies of human performance: The description of human tasks*. Orlando, FL: Academic Press.

Goldernberg, S. (2010, December 2). BP oil spill blamed on management and communication failures. Retrieved from http://www.theguardian.com/business/2010/dec/02/bp-oil-spill-failures

Goodwin, G. F., Essens, P. J. M. D., & Smith, D. (2012). *Multiteam systems in the public sector* (pp. 53-80). Taylor & Francis.

Grimaila, M. R., Schechtman, G., Mills, R. F., & Fortson, L. W. (2009, January). Improving cyber incident notification in military operations. In *IIE Annual Conference. Proceedings* (p. 2357). Institute of Industrial Engineers-Publisher.

Harvey JR. J. C. (2012). *Cyber forces: Commander's cyber security and information assurance handbook*. Department of the Navy: Norfolk, VA.

Illman, P., & Gailey, G. (2012). *Pilot's radio communications handbook sixth edition*. McGraw Hill Professional.

Janis, I. (1972). Victims of groupthink. Boston: Houghton Mifflin.

Johnson, C., Badger, L. & Waltermire, D. (2014) Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150.

Killcrece, G., & Ruefle, R. (2008). Creating and managing computer security incident handling teams (CSIRTs). Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA.

Kohn, L. T., Corrigan, J. M., & Donaldson, M. S. (1999). *To err is human. Building a safer health system*. Committee on Quality of Health Care in America. Washington, DC: Institute of Medicine.

Kozlowski, S. W., & Ilgen, D. R. (2006). Enhancing the effectiveness of work groups and teams. *Psychological Science in the Public Interest*, *7*(3), 77-124.

Ministry of Security and Justice, the Netherlands; Federal Office for Information Security, Germany; Swedish Civil Contingencies Agency, Sweden. (2014). *International case report on cyber security incidents: Reflections on three cyber incidents in the Netherlands, Germany and Sweden.*

Nelson, J. K., Zaccaro, S. J., & Herman, J. L. (2010). Strategic information provision and experiential variety as tools for developing adaptive leadership skills. *Consulting Psychology Journal: Practice and Research, 62*, 131-142.

NICE. (2013). The national cyber security workforce framework 1.0. Retrieved from http://csrc.nist.gov/nice/framework/national_cyber__security_workforce_framework_03_2013_version1_0_for_printing.pdf

Rashid, F.Y. (2015) Cybersecurity has a leadership problem: Study. Security Week. Retrieved from http://www.securityweek.com/cybersecurity-has-leadership-problem-study.

Reinhardt, W., Schmidt, B., Sloep, P., & Drachsler, H. (2011). Knowledge worker roles and actions—results of two empirical studies. *Knowledge and Process Management*, *18*(3), 150-174.

Scott. B. C. (2012). Broadening army leaders for the volatile, uncertain, complex and ambiguous environment. Unpublished master's thesis, U.S. Army War College, Carlisle, PA.

Shappell, S.A., and Wiegmann, D.A. (1996). U.S. naval aviation mishaps 1977-92: Differences between single- and dual-piloted aircraft. Aviation, Space, and Environmental Medicine, *67*, 65-9.

Steiner, I. D. (1972). *Group processes and productivity*. New York: Academic Press.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., ... & Tetrick, L. E. (2015). Improving cyber security incident response team effectiveness using teams-based research. *Security & Privacy, IEEE,13*(4), 20-29.

Stiehm, J.H. (2002). *The U.S. Army War College: Military education in a* *democracy*. Philadephia, PA: Temple University Press.

Studdert, D. M., Brennan, T. A., & Thomas, E. J. (2002). What have we learned from the Harvard Medical Practice Study? In M. M. Rosenthal &K.M. Sutcliffe (Eds.), Medical error: What do we know? What do we do? (pp. 3–33). San Francisco: Jossey-Bass.

The Swedish Civil Contingencies Agency. (2012). Reflections on civil protection and emergency preparedness during major IT incidents: A study of societal impact following the disruption at Tieto in November 2011 (Publication No. MSB 435-12). Retrieved from: https://www.msb.se/RibData/Filer/pdf/26243.pdf

U.S. Department of Defense, National Guard. (2005). After action review: Hurricane response. September 2005 (NGB J7).

U.S. Department of Homeland Security, Federal Emergency Management Agency. (2005, September 30). Urban search and rescue operations completed: Hurricane Katrina urban search and rescue teams are due to return home. Retrieved from https://www.fema.gov/news-release/2005/09/30/urban-search-and-rescue-operations-completed.

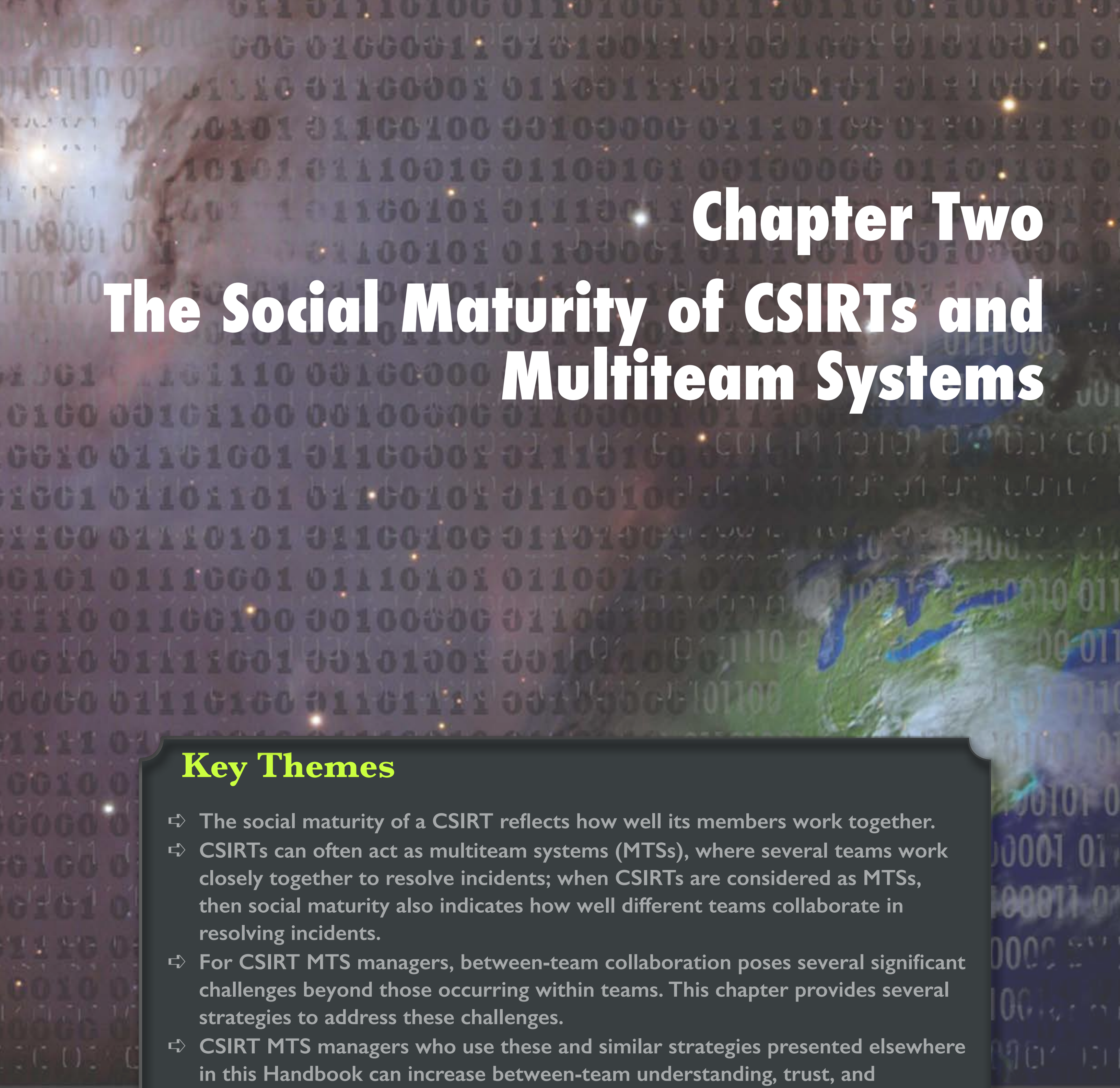
U.S. Executive Office of the President, U.S. Assistant to the President for Homeland Security and Counterterrorism. (2006).*The Federal response to Hurricane Katrina: Lessons learned*. (PREX 1.2:K 15) Washington, D.C.: White House.

Wertheimer, M. (1954). *Productive thinking*. New York: Harper & Row.

West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). *Handbook for computer security incident response teams (CSIRTs) (2nd Ed.)*. Carnegie Mellon Software Engineering Institute: Pittsburgh, PA.

Wolf, L. J. (2004). Can you handle the headaches? Analyzing and optimizing the effectiveness of the incident management process. *Information Systems Security*, *13*(5), 9-20.

Zaccaro, S. J., Marks, M. A., & DeChurch, L. (Eds.). (2012). *Multiteam systems: An organization form for dynamic and complex environments*. Routledge.



Chapter Two
The Social Maturity of CSIRTs and Multiteam Systems

Key Themes

- The social maturity of a CSIRT reflects how well its members work together.
- CSIRTs can often act as multiteam systems (MTSs), where several teams work closely together to resolve incidents; when CSIRTs are considered as MTSs, then social maturity also indicates how well different teams collaborate in resolving incidents.
- For CSIRT MTS managers, between-team collaboration poses several significant challenges beyond those occurring within teams. This chapter provides several strategies to address these challenges.
- CSIRT MTS managers who use these and similar strategies presented elsewhere in this Handbook can increase between-team understanding, trust, and collaboration.

Contents

2.0 Introduction

This Handbook is intended to provide insight and recommendations on how to enhance the abilities of cybersecurity incident responders to work well together. In this chapter, we expand on the social nature of cybersecurity incident response. We describe the social components of strong CSIRT collaboration, and we introduce the concept of CSIRTs as Multiteam Systems (MTSs; Chen, et al., 2014).

2.1 Why are Effective Social Dynamics Important in CSIRTs?

In Chapter 1 ("Introduction to the Handbook"), we noted that two of the research themes that serve as a foundation for this Handbook are that (a) incident responders need to work in complex environments, and (b) the nature of CSIRT work is *knowledge work*. Incident responders work under conditions of very high information load, handling tremendous streams of data and information. While most events and incidents require routine responses, on occasion, some events will turn out to be highly impactful and threatening incidents. In such instances, there is also greater time urgency, as speed of response and remediation becomes critical. The resolution of these incidents entails knowledge work, where analysts engage in thinking and problem-solving to come up with solutions and strategies.

For routine and low impact incidents, the generation and implementation of a solution often can be completed by a single analyst. However, when incidents become more complex, novel, time-urgent, and/or highly impactful, analysts will likely need to work with other incident responders. The complexity and novelty of some incidents require multiple people having different kinds of expertise and experiences thinking together (i.e., engaging in *collective knowledge work*) to generate the best or most appropriate solution. The effectiveness of a CSIRT is determined not so much by how well they handle the routine aspects of incident response, but rather by how successfully and quickly they resolve or mitigate the unusual and extraordinary incidents and threats. Thus, *high performing and high quality CSIRTs are those that have the capacity to work well together, those that have high levels of social maturity*.

High performing and high quality CSIRTs are those that have the capacity to work well together, those that have high levels of social maturity.

2.1.1 THE ELEMENTS OF SOCIAL MATURITY IN CSIRTS

A number of maturity models have been introduced recently into the CSIRT literature (Butkovic & Caralli, 2013; NCSC-NL, 2015; Stikvoort, 2010). CSIRT maturity has been defined as:

> An indication of how well a team governs, documents, performs, and measures the CSIRT services. Is the CSIRT aware of the various processes and the required steps? Are these written down, shared, examined, and improved? Is it clear what the CSIRT authority and accountability is? Are there mechanisms to ensure that the CSIRT follows the formal processes and adequately serves its constituency? Are there mechanisms in place to constantly learn and improve? (NCSC-NL, 2015, p. 2)

The National Cyber Security Centre in the Netherlands (NCSC-NL) defined five areas that contribute to CSIRT maturity levels: Foundation, Organizational, Human, Tools, and Processes. In this chapter, we will focus on the human area. More information about the entire maturity model can be found at:

www.gccs2015.com/sites/default/files/documents/CSIRT%20Maturity%20Toolkit%2020150409.pdf

According to the NCSC-NL CSIRT maturity model, the human area refers to the skills and capacities of the CSIRT members: "Finding the right people for your team, training them well, and keeping them for at least a number of years for maximum efficiency is crucial to the success of your CSIRT" (NCSC-NL, 2015, p. 10). This area includes such aspects as codes of ethical conduct, size requirements of a team to foster team resilience, members' skills, training programs, and external networking activities. Thus, according to this model, key questions managers can ask to assess CSIRT maturity in this area are (CSIRT Maturity Kit, n.d., p. 2):

- *"What is the minimum staffing required to function?"*
- *"Is there an official 'code-of-conduct'?"*
- *"Do we have a clear policy for training our team members?"*
- *"Are we connected to the right (social) networks?"*

These parameters are indeed essential to constituting a functioning CSIRT with the necessary size and skills to accomplish incident response. However, organizational psychologists have long acknowledged that member capacities and team size are not enough to maximize team effectiveness and success. Members also need to develop *the capacity to collaborate well together* in accomplishing the team's mission to develop an effective *synergy* among team members. We would define such synergy as reflecting the ***social maturity*** of a CSIRT.

Our focus group interviews suggested that a number of critical elements contribute to the social maturity of a CSIRT. These are:

- Do team members know when and how to trigger collaboration activities among CSIRT members in response to

CSIRT social maturity reflects how well members communicate and share information with one another, how well they solve problems together, how much knowledge and trust they share, how well they adapt and learn as a team, and how well they manage any conflict among themselves.

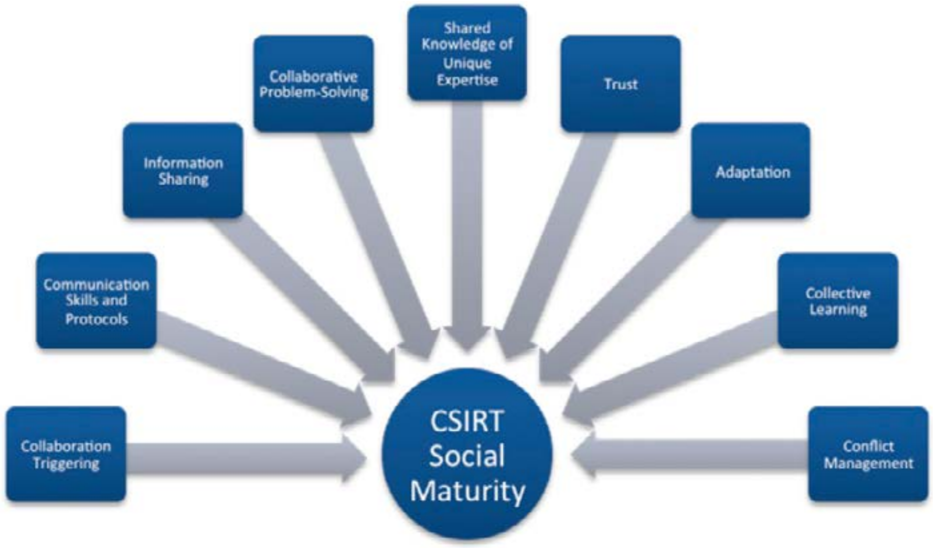
particular events?

- Does the CSIRT have the correct shared communication norms and protocols to ensure effective and timely sharing of information? Do members have the communication skills to work well within these protocols?
- Do members collaborate effectively in all stages of CSIRT problem-solving?
- Do CSIRT members have a shared understanding of who has what unique set of experiences and expertise in the team?
- Do members of the CSIRT trust one another?
- How well does the CSIRT adapt (cognitively and behaviorally) to novel and changing circumstances?
- How well does the CSIRT learn from failures and new experiences?
- How well does the CSIRT manage internal conflict?
- How well does the CSIRT manage conflict with external stakeholders?

> **Every time we talk about how we operate, we're trying to push that it's not five teams. Anything we do generally involves every single one of those teams, so there's no real concept of this isn't an incident handling problem, this is an international team problem; no one team can survive on their own. They've got to rely on all the other teams.**
>
> **~CSIRT Manager**

Figure 2.1 summarizes these elements of CSIRT social maturity. While they can each be defined in terms of teamwork skills possessed by individual CSIRT members, they also reflect the quality of interactions among team members. CSIRT social maturity reflects how well members communicate and share information with one another, how well they solve problems together, how much knowledge and trust they share, how well they adapt and learn as a team, and how well they manage any conflict among themselves. A key task for CSIRT managers to maximize the performance of their teams is to create the conditions for these elements to flourish.

Figure 2.1 Elements of CSIRT Social Maturity



Each element in Figure 2.1 is described in one or more of the other chapters in this handbook. For each one, we provide a set of strategies and recommendations managers can use to improve their teams. We also provide an assessment exercise that can be used by managers to evaluate the state of their teams on each element. These assessments can be used specifically to evaluate social maturity levels in similar ways to how CSIRT maturity models such as SIM3 assess CSIRTs more generally (https://check.ncsc.nl/static/CSIRT_MK_brochure.pdf; Stikvoort, 2010). We will describe the use of these assessments later in this chapter.

> **There's always tension between public and private [teams] because in the center, we speak about national security or instability in society where the business, private companies talk about business continuity. That's the most important thing for them. So you have to connect those two things together unless you have shared interests. If you have shared interests, there's no conflict. So you have to find common interests.**
>
> **~CSIRT Manager**

2.2 CSIRT Multiteam Systems

The current literature on the human element of CSIRT maturity has an exclusive focus on the quality of a team. However, cybersecurity incident response often involves the action of multiple teams working closely together. In this Handbook, we refer to this arrangement as a multiteam system (MTS; Chen, et al., 2014; Zaccaro, Hargrove, Chen, Repchick, & McCausland, 2016). A critical point for CSIRT managers is that social maturity of a CSIRT reflects not only how members work well as a team, but also how well the team works closely with other teams.

2.2.1 WHAT IS A MULTITEAM SYSTEM?

Organizational scientists have defined an MTS as a closely connected network of teams working together to accomplish a common goal (Mathieu, Marks, & Zaccaro, 2001). Most organizations contain collections of teams, but these are not necessarily considered MTSs. What differentiates an MTS from these other kinds of arrangements is that the teams in an MTS interact and work closely together – much as members of a single team would – when completing a task or mission. Teams within an MTS are called *component teams*.

Organizational scientists describe four levels of interaction, or interdependence, which can occur between teams in an organization (Tesluk, Mathieu, Zaccaro, & Marks, 1997):

1. *Pooled actions:* Teams work independently from one another, with little or no interaction required among them.
2. *Sequential Interactions*: Teams complete actions on a task and then pass the results to another team to work on. Interaction flows from one team to another.
3. *Reciprocal Interactions*: Teams complete an action on a task and pass the task to another team; that team returns the results of its work back to the original team. Teams can work through several iterations until the task is completed.
4. *Intensive Interactions*: Multiple teams interact with one another in the same time and space to resolve a problem.

Most teams in organizations engage in pooled or sequential interactions. However, teams that are working as part of an MTS typically engage in reciprocal or intensive interactions with other teams in the system.

2.2.2 MTS GOAL HIERARCHIES

All component teams in an MTS work toward a common, overarching goal called the *distal goal*. However, individual teams may work by themselves or with 1-2 other teams to accomplish a more immediate goal, called a proximal goal. As the MTS gets closer to accomplishing the distal goal, more component teams become involved in the overall MTS mission. Thus, the goals of different component teams working in an MTS can be defined as a hierarchy of *proximal goals* contributing to the accomplishment of the *distal goal*.

Table 2.1 shows an example of a CSIRT goal hierarchy that may occur in an MTS when a potentially severe threat is detected. A watch or network monitoring team is typically responsible for detection of possible malicious activity (goal 1). For threats that are non-routine or complex, that team may work with the

> **I think that's a great depiction of how it works within [our team]. I think there's also the project side of what we do. And a lot of times, you're dependent upon resources and teams that are outside of corporate. So you depend on people out in the business who probably don't share the same set of priorities you do.**
>
> **~CSIRT Manager**

forensics, malware, and threat intelligence teams to accomplish the determination of the incident's nature and threat parameters (goal 2). This is a shared proximal goal for these three teams. The forensics and/or malware analysis teams would then work with an operations team on the proximal goal of threat eradication from the network (goal 3). The next proximal goal of sharing and communicating threat intelligence information is accomplished by the threat intelligence and communications teams working together (goal 4). Finally, the distal goal of re-establishing a secured cyber environment (goal 5) is accomplished by the integrated efforts of communications, security policy and strategy teams, along with CSIRTs and stakeholder teams from other companies.

The MTS goal hierarchy is not the same as process models that are common in the CSIRT literature (e.g., Alberts, Dorofee, Kilcrece, Ruefle, & Zajicek, 2004; Maj, Reijers & Stikvoort, 2010). Process models specify a series of steps or behaviors (i.e., the tasks) that individual analysts or teams typically enact when completing an action. The MTS goal hierarchy indicates the *goals* that teams working together must accomplish. Different teams may complete their own series of process steps to carry out their particular functions, but goal accomplishment in MTS hierarchies is the result of several component teams within the CSIRT engaging in these or other processes together to reach certain stages of cybersecurity incident response.

2.2.3 INTERNAL VERSUS EXTERNAL MTSs

Organizational scientists distinguish between *internal* and *external* MTSs (Mathieu, et al., 2001). An internal MTS is one in which all of the component teams come from the same organization. An external MTS is one in which component teams come from different organizations. Larger organizations typically have mostly internal CSIRT MTSs. Smaller companies, or those that do not have the resources to create a larger internal MTS, may establish one or two component teams (e.g., monitoring and response teams), but rely on outside organizations for such functions as forensics, malware analysis, and threat intelligence. Or, companies may establish a CSIRT composed of individuals who perform most CSIRT functions but call in other support groups when high impact or high severity incidents attack the company. Both of these arrangements are examples of external CSIRT MTSs. Likewise, even when an organization has an internal MTS, high severity threats may require bringing in outside legal teams and external customer/stakeholder teams. In such instances, the internal MTS becomes an external MTS.

Internal and external MTSs can pose different challenges for incident response managers. Both types of MTSs require managers to focus on facilitating collaboration (a) within each of the component teams, ***and*** (b) between all of the component teams working together on specific proximal goals. Component teams in an internal MTS share the same organizational norms, values, and expectations. This may not be true in external MTSs, causing greater between team conflict and mistrust. Later in the chapter, we provide some management strategies to facilitate collaboration in such circumstances.

2.2.4 FORMING CSIRT MTSs

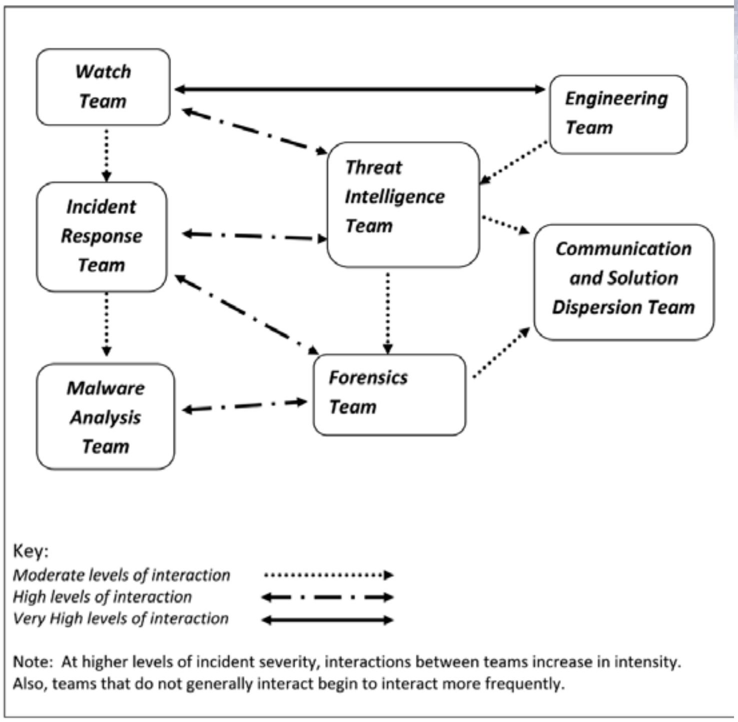
Types of CSIRTs vary in terms of their size and the permanence of their structures (Zaccaro, Marks, & DeChurch, 2012). The choice of which type to establish often is determined by the amount of resources that can be devoted to cybersecurity response, the overall size of the organization, the frequency of high impact and severe incidents threatening the organization, and the sensitivity of its data (e.g., organizations in critical infrastructure sectors such as financial, health, military, government, and utilities).

Organizations can form different types of CSIRTs that reflect different forms of MTSs. These include:

- A permanent larger MTS that includes component teams related to network monitoring, incident response, forensics, malware analysis, engineering, intelligence, and communications teams.

TABLE 2.1 AN EXAMPLE OF AN INCIDENT RESPONSE MTS GOAL HIERARCHY (ADAPTED IN PART FROM ZACCARO, ET AL., 2016)

STEPS IN A MULTITEAM SYSTEM GOAL HIERARCHY	COLLABORATING COMPONENT TEAMS
1. Detection of malicious activity (*proximal goal*)	• Network Monitoring Team
2. Identification of event nature and parameters (*proximal goal*)	• Network Monitoring Team • Forensics/Malware Analysis Team • Threat Intelligence Team
3. Threat eradication from network (*proximal goal*)	• Forensics/Malware Analysis Team • Operations Team
4. Threat intelligence communication (*proximal goal*)	• Threat Intelligence Team • Communications Team
5. Secured cyber environment (*distal goal*)	• Communications Team • Security Policy and Strategy Team • External CSIRTs and Stakeholder Teams


Watch Team
Engineering Team
Threat Intelligence Team
Incident Response Team
Communication and Solution Dispersion Team
Malware Analysis Team
Forensics Team
Key:
Moderate levels of interaction
High levels of interaction
Very High levels of interaction

Note: At higher levels of incident severity, interactions between teams increase in intensity. Also, teams that do not generally interact begin to interact more frequently.

Figure 2.2 Example of a Cybersecurity Incident Response Multiteam System

- A permanent smaller MTS composed of monitoring and incident response teams that handles relatively routine incidents but may occasionally call in other teams on an as-needed basis depending on the nature and potential impact of severe incidents. Established protocols determine when such teams are brought into the MTS.
- An ad hoc MTS composed of a team of analysts who handle most incident response functions but call in other teams specializing in forensics, malware analysis, communications, and legal issues on an as-needed basis.

We describe next some of our research findings that point to both similarities and differences among CSIRT MTSs based on CSIRT type.

TABLE 2.2 COMPONENT TEAMS IN A TYPICAL LARGE MTS CSIRT

TEAM NAME	TEAM FUNCTION
Watch Team	"Eyes on glass." Team members monitor computers and networks for incidents and flag unusual patterns. Escalate incidents to the next levels of analysis.
Incident Response Team	This team creates, tracks, and assigns incidents. Acts as a single point of contact for incident resolution. Team members receive notification of incidents and triage them. Resolution is generally rapid, coordinated incident response. These teams will typically provide on-site response support.
Malware Team	Team members reverse engineer the malware to get to the "why did this happen?" Investigate deeper than surface level containment of the incident. Goal is to build something better than what they just reverse-engineered.
Forensics Team	Team members deeply analyze artifacts and media to determine the nature of, and assist with scoping, the incident. Provides indicators of compromise (IOCs) and possible mitigation information for use by network defenders.
Threat Intelligence & Analysis	Team members take a longer view, create and integrate information from internal and external sources that can be used by teams to better understand the threat, handle incidents, and perform analysis and mitigation activities. They are a resource to be used by the other teams and do research/projects in order to be proactive. Take knowledge from incidents that can be researched and expanded upon. Build tools to help the incident response teams (e.g. security tools and intrusion detection services).
Engineering	This team works as IT support to the entire system. Designs software, configures and maintains security and IT tools.
Communications Team	This team prepares and sends out knowledge documents to promote threat and solution awareness.

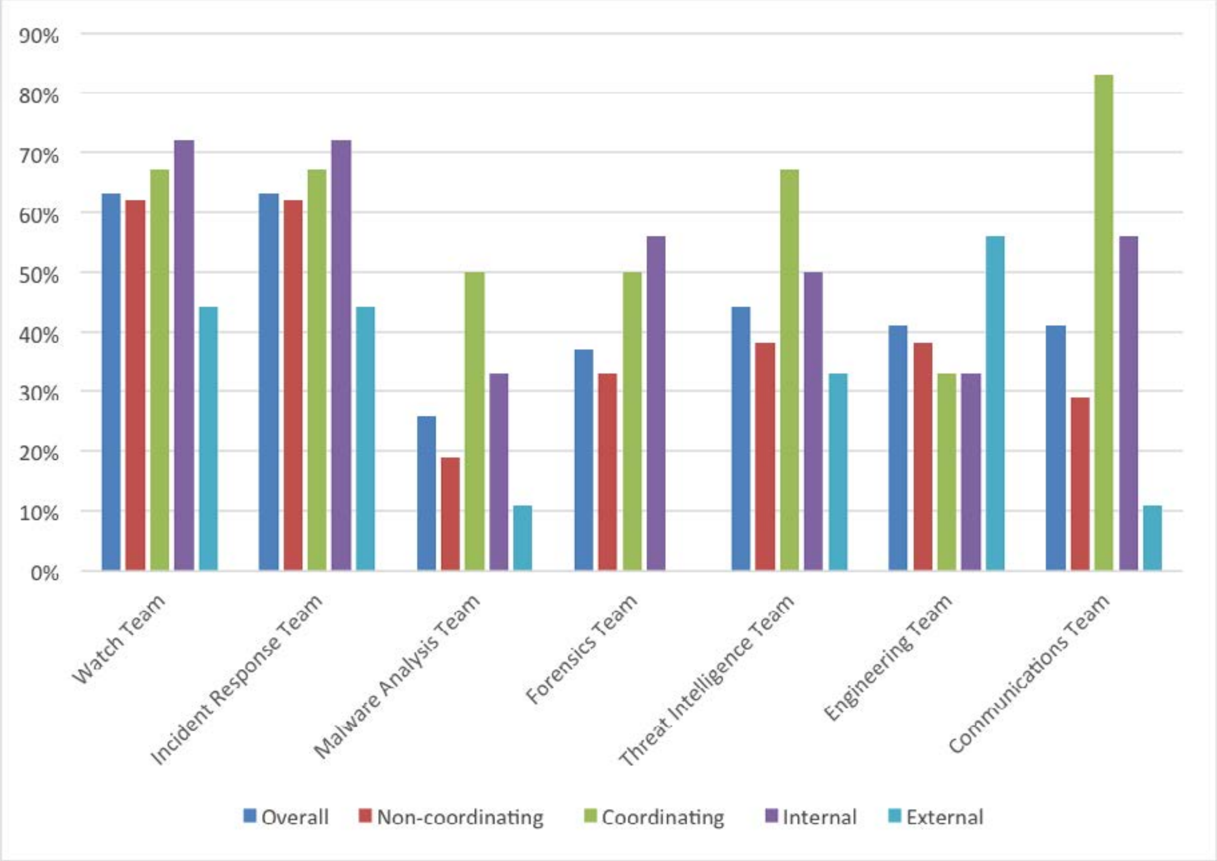


Figure 2.3 Frequency of all 7 Typical Teams Across 28 CSIRTs

2.3 Project Findings: Typical CSIRT MTSs

As part of our focus groups, we interviewed managers who represented 28 CSIRT MTSs of differing types. Coordinating CSIRTs "facilitate the handling of incidents, vulnerabilities, and general information across a variety of external and internal organizations" (Bhaskar, 2005, p. 5); whereas, we define non-coordinating CSIRTs as CSIRTs that may be internal or external to the organization. Internal CSIRTs are categorized as those whose constituency is the organization that directly employs the CSIRT personnel, and external CSIRTs are synonymous with what many know as managed security service providers that provide CSIRT services for a fee to other organizations other than those who employ the CSIRT personnel directly. [1] Figure 2.2 displays a typical MTS structure that was derived from interviews. This MTS contains 7 component teams. Table 2.2 lists these teams along with their generic functions. Note that not all of the MTSs we examined included all of these teams, and several of them had different names across companies. However, most of these teams were represented in larger CSIRT MTSs. In smaller CSIRTs, a single team generally contained members who accomplished several of these functions. However, such teams would contract outside services in cases of severe threats. In total, we interviewed 28 MTSs. Of those, 6 were coordinating CSIRTs. 15 of the 28 were classified as internal CSIRTs, while 7 were classified as external CSIRTs.

Figure 2.2 shows how interaction patterns differ across component teams in a typical MTS. Some teams work very closely with one another (e.g., watch and engineering teams); other teams rarely work together (e.g., watch and forensics teams). However, many CSIRT MTS managers noted that these interaction patterns changed as incident severity increased. Teams engage in more intense interactions with one another when resolving high impact and high severity events. Also, teams that do not generally work together begin doing so in cases of high impact threats.

Figure 2.3 indicates how many CSIRTs that we interviewed had a team for each of the seven functions we found. These data are

[1] In our summary of MTSs from our interviews, we also included two ad hoc CSIRTs in the non-coordinating category even though in the strictest sense these CSIRTs only become MTSs during certain incidents. Both of these CSIRTs were academic CSIRTs that have a core CSIRT team with people who perform different functions, and then coordinate with other teams within the employ of the academic institution (but outside of their immediate group) on an as-needed basis.

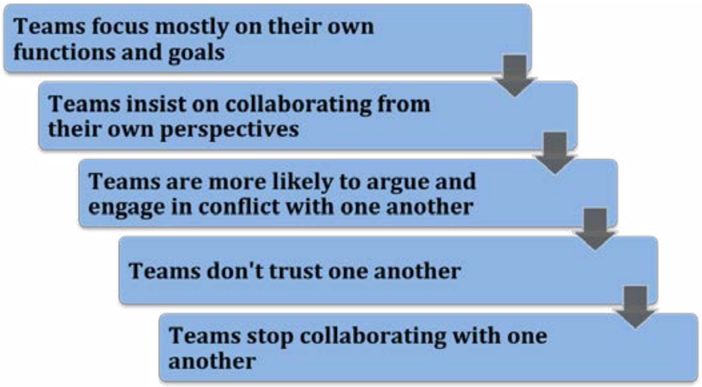
> **“My forensics guys are completely different than my incident handlers because they require different things. I mean, forensics means that you're going to take six months to make sure that we have a thorough and complete answer here. Incident response, you don't have time for that. It's pull this next. Drop that machine. Destroy that machine. Tear this thing down. It's done, right? So they never get along. …when I first had them in the lab, my incident response guys literally walled themselves away from the forensics team. I mean, with the cubes. Like, they would not -- they didn't want to associate with each other.”**
>
> **~CSIRT Manager**

further broken down by type of CSIRT (e.g. internal versus external; coordinating versus non-coordinating). While the sample sizes are small, some of the larger differences in percentages suggest that:

- Coordinating CSIRT MTSs are more likely to include a communications team than non-coordinating CSIRT MTSs.
- Coordinating CSIRT MTSs are more likely to include a malware analysis team than non-coordinating CSIRT MTSs.
- Coordinating CSIRT MTSs are more likely to include a threat intelligence team than non-coordinating CSIRT MTSs.
- Internal CSIRT MTSs are more likely to include all of the component teams, except an engineering team, than external CSIRT MTSs.

Interviews with CSIRT MTS managers also indicated that teams in coordinating CSIRT MTSs tended to display higher levels of interactions, and these interactions involved greater numbers of the component teams working together.

Figure 2.4 Challenges in CSIRT MTS Collaboration


Teams focus mostly on their own functions and goals
Teams insist on collaborating from their own perspectives
Teams are more likely to argue and engage in conflict with one another
Teams don't trust one another
Teams stop collaborating with one another

2.4 Challenges in Managing MTSs

Our research findings indicate that MTSs are common in the domain of cybersecurity incident response. We noted earlier in this chapter that the social maturity of a CSIRT reflects how well members of a single team work together. However, when CSIRTs are considered an MTS, then social maturity also indicates ***how well different teams collaborate in resolving incidents***. For CSIRT MTS managers, between-team collaboration poses several significant challenges beyond those occurring within teams. Figure 2.4 shows a pattern of team actions that occur in many poor performing MTSs.

- *Teams generally focus on their own functions and goals:* Component teams in a CSIRT MTS will have their own functions and goals. Those goals will generally take precedence over those shared with other teams. For example, a malware analysis team may be more concerned with discovering the capabilities of a malware sample as opposed to how it was initially introduced into an organization’s computer system. A similar problem can happen when product developers insist on repeated testing, while sales departments insist on getting a product to market as quickly as possible.
- *Teams insist on collaborating from their own perspectives:* Because component teams have different functions, they bring different perspectives to cybersecurity incident response. While this can be good when engaging in collaborative problem solving (see Chapter 7), teams will often tend to see a problem only from their own perspective.
- *Teams are more likely to argue and engage in conflict with one another:* If teams that bring different perspectives to a problem insist on their own viewpoint, harmful conflict will occur more often in the CSIRT MTS.
- *Teams don’t trust one another:* As conflict increases between teams in a CSIRT MTS, they begin to trust one another less.
- *Teams stop collaborating with one another:* When component teams lose trust in one another, they stop collaborating, and overall MTS effectiveness declines.

This pattern is a common one in many CSIRT MTSs, especially those (a) with a greater number of component teams, or (b) ad hoc in nature, coming together only for severe incidents. A major task for CSIRT managers and top management leadership, then, is to promote collaboration not only within each component team in their MTS but also to facilitate effective collaboration among their teams.

2.5 Strategies for CSIRT MTS Managers

Managers can take a number of steps to increase the effectiveness of their MTSs. The recommendations we offer below are designed to (a) help you understand your CSIRT as an MTS, and (b) facilitate the efforts of your teams to work well with one another.

Recommendation 1: Map your MTS

Effective CSIRT MTS leadership requires that managers:

- Understand their CSIRT as a connected set of teams;
- Be aware of the different degrees of interaction typically occurring between their teams; and
- Be aware of how these interactions change under conditions of higher impact or more severe events.

Addendum 2.1 and Appendix E contain a template that managers can use to map their MTS and show the typical interactions that occur among their teams. To use this template, list each team in your MTS in the first column. Repeat this listing again along the top row, minus your last team in the first column. In each cell, use the key provided to indicate the typical interaction that occurs between teams and the interactions that occur during higher severity incidents. An example of how to complete this template is included in Addendum 2.1. This template can help you determine where you need to manage team collaborations more closely, especially when incidents increase in severity. After completing this template for his/her CSIRT MTS, the manager will become aware of which teams have the highest interaction patterns. The manager would then expend the most resources to address collaboration needs for those specific teams (e.g., plan a scenario-based training for these specific groups).

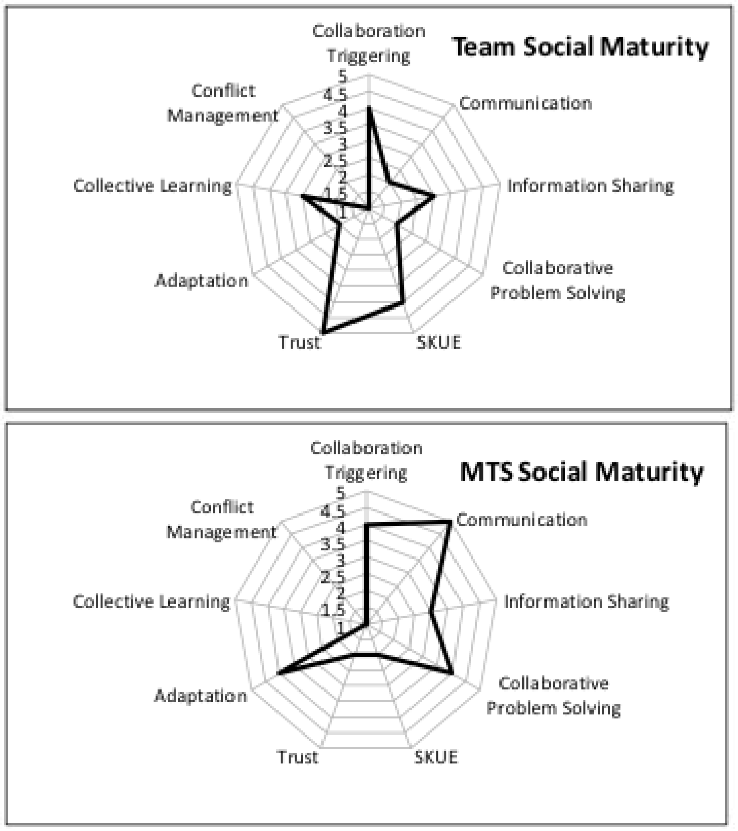


Figure 2.5 Assessment of CSIRT Social Maturity in a Team and an MTS
SKUE = Shared Knowledge of Unique Expertise

Recommendation 2: Assess the Social Maturity of Each CSIRT Component Team and Overall CSIRT MTS

Earlier, we defined CSIRT social maturity as the degree to which a team has the capacity for its members to collaborate and work well together in completing the team's mission. We argue that such maturity reflects high levels of:

- Collaboration triggering
- Communication skills and protocols
- Information sharing
- Collaborative problem solving
- Shared knowledge of unique expertise
- Trust
- Adaptation
- Collective learning
- Conflict management

To have full social maturity, these attributes should not only occur within component teams in an MTS, but also between component teams and across the entire CSIRT MTS. In the chapters that follow this one, we describe each of the elements of CSIRT social maturity, and we provide assessment exercises with a response score on a 1-5 scale to help a manager evaluate the level of a particular element in his or her component team or CSIRT MTS. These exercises are also included as a set in Appendix B. Managers can use the score from each set of chapter assessment exercises to create radar diagrams similar to those used in other CSIRT maturity models to assess levels of social maturity. Figure 2.5 provides an example of a radar diagram for a team and one for a CSIRT MTS. The team diagram refers to social dynamics within a single team and can be used by team leads. The MTS diagram refers to social elements among teams and across a CSIRT MTS. Managers can use both diagrams to assess the social maturity of the entire CSIRT MTS.

This Handbook contains a number of strategies and recommendations for improving each of the elements of CSIRT social maturity for both teams and CSIRT MTSs. Another strategy that CSIRT MTS managers can use to facilitate their teams working well with one another is to hire team members who have a preference for working in teams.

Recommendation 3: Make Team Staffing Decisions by using Situational Interviews to Assess Group Work Preference

Situational interviewing is a technique used to encourage job applicants to describe how they have handled specific work situations in the past. The interviewer asks job candidates a predetermined, standard set of questions focused on past behaviors and experiences that will enable interviewees to showcase the knowledge, skills, or abilities they will need to be successful on the job (Pulakos & Schmitt, 1995). The key to situational interviewing is the underlying notion that past performance in similar situations predicts future performance (Latham, Saari, Pursell, & Campion, 1980). Asking job candidates how they have solved problems and handled past challenges that they are likely to also encounter on the job will determine if the candidate has the experience to be successful.

Recommendations for use:

- Use situational interviewing techniques when selecting potential new CSIRT members. Ensure that all interviewees receive the same questions so that responses can be compared directly.
- Determine the team- and cross-team-related situations that are most critical to CSIRT success and that the new team member is most likely to encounter on the job. Use these situations as the basis for possible questions.
- To create situational interview questions that measure a preference to work in teams, write ones that address the specific ways a team member needs to work with other teams in the position for which you are hiring. The questions you write should give applicants the opportunity to describe how they handled a specific situation in the past and to describe the outcome of their actions, enabling you to infer how they would handle a similar situation on your CSIRT.
- When scoring responses to situational interview questions, have two interviewers in the room. Both should rate the response on a 1-5 scale (1 being poor; 5 being excellent) and then discuss their reasons for assigning a particular score. Interviewers may find it helpful to take notes during the interview to more easily remember the exact reasons for assigning a particular score.

Situational Interview Sample Questions and Responses

We have designed the following sample questions as suggestions for assessing an applicant's preference for group work. These questions help managers assess a characteristic that will determine which applicants prefer to work in groups and will choose to collaborate rather than working independently. CSIRT managers can use these questions to determine whether applicants would have a natural tendency to collaborate within their own team in the CSIRT and across teams. Please note that the situational interview questions below have not undergone the necessary rigorous validation process (see Appendix C, "Hiring and Training CSIRT Employees: Validation Considerations"). They are only intended to provide CSIRT managers with an idea for the types of situational interview questions that can be used to measure applicant preference for group work. Managers should refer to their Human Resource Management departments for additional information about validation of such items.

Question 1: Describe a situation in which you had to make a decision on whether you wanted to solve an incident alone or involve others. How did you make the choice to involve others (or not) and what factors did you consider? Be as specific as possible describing the incident, and your thought process.

ELEMENTS OF STRONG RESPONSES	RED FLAG RESPONSES
• Includes all of the details necessary to understand that response (i.e. description of situation, the background, and the factors that went into the decision to collaborate)	• Lacks complete details of the situation (i.e., description of choice is vague, unrealistic or not a real choice)
• When in doubt, chooses to collaborate with others	• When in doubt, chooses not to collaborate with others
• Clearly demonstrates a preference for working with others in an ambiguous situation	• Demonstrates a preference to work alone, rather than with others, in an ambiguous situation
• Makes a choice to collaborate and doesn't collaborate solely because of a procedure in place	• Makes a choice not to collaborate, even when collaboration is useful
• Describes specific factors that went into the collaboration decision	• Provides a vague response when describing the factors that went into the decision

Question 2: Describe a situation in which you had to make a choice between finishing a task quickly on your own or taking the time to involve your CSIRT so the entire group would benefit and

ELEMENTS OF STRONG RESPONSES	RED FLAG RESPONSES
• Includes all of the details necessary to understand the situation (i.e. description of situation, the background, and the choice that the applicant had to make)	• Lacks complete details of the situation (i.e., description of choice is vague, unrealistic or not a real choice)
• Provides a situation where the choice was to involve others in the CSIRT, so the entire group would benefit	• Provides a situation where the choice was to finish the task alone
• Mentions the importance and/or benefit of working with others	• Mentions it is more important to finish task quickly and does not mention that information was shared
• Provides details that demonstrates a preference to work for the group rather than working alone	• Details of response indicates that the applicant would likely prefer to work alone than work with others

learn. What did you do to reconcile those two conflicting choices and what actions did you take? Be as specific as possible in your description of the situation and the choices that you made.

While situational interview questions don't have wrong answers, the elements of strong responses and the red flag responses above should help in the scoring of applicant responses to questions and differentiate between the strong and weak preferences to work in teams of various job applicants.

Recommendation 4: Focus on emphasizing distal goal commitment

The following two recommendations (Recommendations 4 and 5) can help managers address the broader challenges that can harm CSIRT MTS performance (see Figure 2.4). As suggested in Figure 2.4, component teams in a CSIRT MTS tend to focus more on their own functions, missions, and goals than on those shared with other teams. Managers can counteract this tendency *by emphasizing common or shared goals*. For example, an engineering team may be too focused on developing a new piece of software or configuring a new system to collaborate effectively with a threat intelligence team that is trying to eradicate a particular threat. A manager would work with the engineering team lead to refocus the team toward threat resolution without losing the emphasis on its core mission. This managerial approach rests on increasing shared goal cooperation among teams. Studies have demonstrated that such goal cooperation increases open-mindedness and knowledge creation in teams (Mitchell, Boyle, & Nicholas, 2009). One study with product research and development (R&D) MTSs showed that MTSs with higher shared goal commitment displayed better inter-team coordination (Hoegl, Weinkauf, & Gemuenden, 2004).

Recommendation 5: Encourage regular cross-team connections

Component teams in an MTS tend to communicate mostly among themselves and less often with other teams. Such communication patterns lessen knowledge about, and trust in, other teams. They also create misunderstandings about how each team's actions in an MTS are supposed to fit with those of other teams.

Managers can reduce this tendency by creating opportunities for more communication and discussions between different teams. These discussions should focus on the tasks each team is working on and the protocols and standards that drive team actions. In our interviews, CSIRT MTS managers indicated that they encourage such connections by:

- Having regular (weekly, biweekly, or monthly) meetings involving all members of different teams to discuss common tasks and issues;
- Embedding members in different teams for short periods (e.g., 1 week, 1 month, 3 months);
- Establishing regular meetings with team leads;
- Having different teams located physically close to one another, with common spaces for ad hoc meetings during critical incidents;
- Establishing protocols for severe threats that bring together key representatives from different teams to act

> **We know [the] incident response team, because they sit in the same area we do. So, and by their nature we deal with them every day, we see them every day, whereas our interactions with some of the other groups are just general neglect. We never see them, so we don't talk to them.**
>
> **~CSIRT Manager**

> **Something that I had big success with is non-endless shifts. So I forced the engineers to go on the main channel. I forced [another component team] to go on the main channel, eat your own dog food. And I also forced analysts to do [another team's] work. And then for some, it was really like a light bulb going on. And they said, "oh, … this case is horrible that we hand over. That's not enough information, I have to do it all again." And suddenly [they] understood why [this one team] always came to them and said, "hey, analyst, your case quality is bad. What should I do with this?..." They shadow, but they don't do the actual work. So, for example, the engineer sits on the main channel, and the level one analyst sits behind him and watches it. So I did it two hours every two weeks...It fosters the interaction between the teams, of course. Not inside the teams...Yeah, they understand better. The analysts they write requests for the engineers to improve [proprietary system] content. Now they're on the receiving end of this and they see, 'Oh, yeah, now I know what was missing with my question.'**
>
> **~CSIRT Manager**

as a core team to coordinate threat resolution; and/or

- Establishing formal "integrators" on their staffs who were specifically responsible for (a) determining members of different teams that need to work together on a particular incident, and (b) making sure these members come together and have the resources they need to collaborate effectively.

Each of these strategies is intended to increase communications and general information sharing between teams. Managers who use these and similar strategies can increase between-team understanding, trust, and collaboration. There is not sufficient, well-designed research to validate best practices in fostering collaboration between teams in an MTS. However, some initial research has suggested support for these suggestions to enhance MTS collaboration (e.g., Firth, Hollenbeck, Miles, Ilgen, & Barnes, 2014; Hoegl & Weinkauf, 2005).

2.6 Summary

The maturity of a CSIRT depends upon its quality of social dynamics. When CSIRTs are composed of multiple teams, then such maturity reflects not only the strength of collaboration within each team, but also the quality interactions occurring between teams. Accordingly, managers need to attend to both team and MTS effectiveness to increase the overall quality of their CSIRT.

References

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). *Defining incident management processes for CSIRTs: A work in progress* (No. CMU/SEI-2004-TR-015). Software Engineering Institute, Carnegie Mellon University. Retrieved from http://www.dtic.mil/dtic/tr/fulltext /u2/ a453378.pdf

Bhaskar, R. (2005). A proposed integrated framework for coordinating computer security incident response teams. *Journal of Information Privacy and Security, 1*(3), 3-17.

Butkovic, M. J., & Caralli, R. A. (2013). *Advancing cybersecurity capability measurement using the CERT (registered trademark) - RMM Maturity Indicator Lead Scale* (No. CMU/SEI-2013-TN-028). Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Gorab, A. K. (2014). An organizational psychology perspective to examining computer security incident response teams. *IEEE Security & Privacy, 5*, 61-67.

CSIRT Maturity Kit. (n.d.). Retrieved from https://check.ncsc.nl/static/CSIRT_MK_brochure.pdf

Firth, B. M., Hollenbeck, J. R., Miles, J. E., Ilgen, D. R., & Barnes, C. M. (2015). Same page, different books: Extending representational gaps theory to enhance performance in multiteam systems. *Academy of Management Journal, 58*, 813-835.

Hoegl, M., & Weinkauf, K. (2005). Managing task interdependencies in Multi-Team projects: A longitudinal study. *Journal of Management Studies, 42*, 1287-1308.

Hoegl, M., Weinkauf, K., & Gemuenden, H., G. (2004). Interteam coordination, project commitment, and teamwork in multiteam R&D projects: A longitudinal study. *Organizational Science, 15*, 38-55. doi: 10. 1287/orsc. 1030.0053

Maj, M., Reijers, R., & Stikvoort, D. (2010). *European Network and Information Security Agency (ENISA) good practice guide for incident management*. Retrieved from https://www.enisa.europa.eu/activities/cert/support/incident-management

Mathieu, J. E., Marks, M. A., & Zaccaro, S. J. (2001). Multi-team systems. In N. Anderson, D. Ones, H. K. Sinangil, & C. Viswesvaran (Eds.), *International handbook of work and organizational psychology* (pp. 289-313). London: Sage.

Mitchell, R., Boyle, B., & Nicholas, S. (2009). The impact of goal structure in team knowledge creation. *Group Processes & Intergroup Relations, 12*, 639-651.

NCSC, Netherlands (2015). CSIRT Maturity Kit: *A step-by-step guide towards enhancing CSIRT Maturity.* Retrieved from http://www.gccs2015.com/sites/default/files/documents/CSIRT%20Maturity%20Toolkit%2020150409.pdf

Pulakos, E.D., & Schmitt, N. (1995). Experience-based and situational interview questions: Studies of validity. *Personnel Psychology, 48,* 289-308.

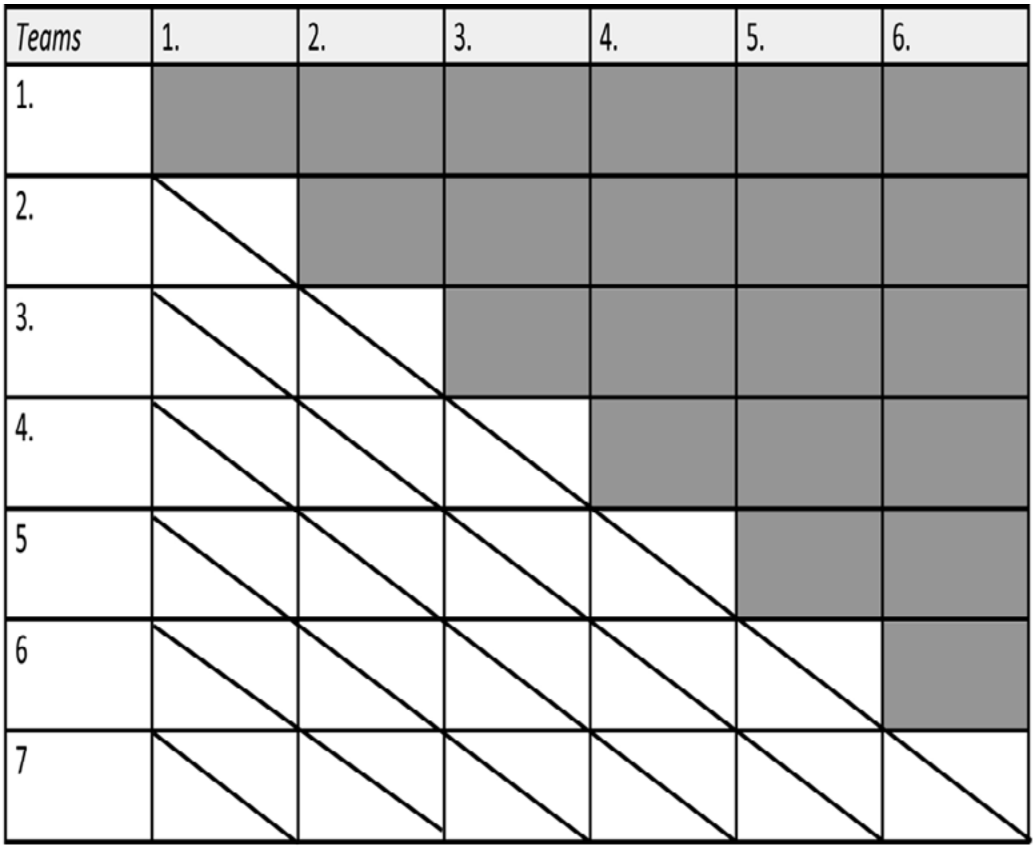
Stikvoort, D. (2010, September 1). *SIM3: Security incident management maturity model*. Retrieved from https://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf

Tesluk, P., Mathieu, J, Zaccaro, S. J., & Marks, M., (1997). Task and aggregation issues in the analysis and assessment of team performance. In M. Brannick, E. Salas, & C. Prince (Eds.), *Team performance measurement and assessment: Theory and application* (pp. 197-224). Hillsdale, NJ: Erlbaum.

Zaccaro, S. J., Hargrove, A., Chen, T., Repchick, K., & McCauseland, T. (2016). A comprehensive multilevel taxonomy of cyber security incident response performance. In S. J. Zaccaro, R. D. Dalal, L. E. Tetrick, & J. Steinke (Eds.), *Psychosocial Dynamics of Cybersecurity (13-55).* New York: Routledge.

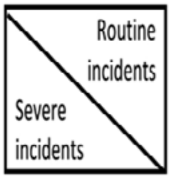
Zaccaro, S. J., Marks, M. A., & DeChurch, L.A. (2012). Multi-team systems: An introduction. In S. J. Zaccaro, L. A. DeChurch, & M. A.Marks (Eds.), *Multi-team systems: An organization form for dynamic and complex environments* (pp. 3-32). London: Taylor Francis/Routledge.

Addendum 2.1 Template for Mapping Your MTS



Teams	1.	2.	3.	4.	5.	6.
1.	▨	▨	▨	▨	▨	▨
2.		▨	▨	▨	▨	▨
3.			▨	▨	▨	▨
4.				▨	▨	▨
5					▨	▨
6						▨
7						

Key: Interaction levels



1. ***Little or no interactions:*** Teams generally work separately
2. ***Moderate levels of interaction:*** One team passes work to the next team
3. ***High levels of interaction:*** Teams pass work back and forth until incident is resolved
4. ***Very high levels of interaction:*** Teams work closely together, often gathering and meeting in the same space.

Instructions

1. In the first column, list each team in your MTS
2. Repeat the list of teams in the top row, skipping team #7
3. In the upper right corner of each cell, using the key to indicate the typical or routine levels of interaction between the two teams
4. In the lower left corner of each cell, using the key to indicate the levels of interaction occurring between the two teams during high impact of severe cyber incidents.

EXAMPLE

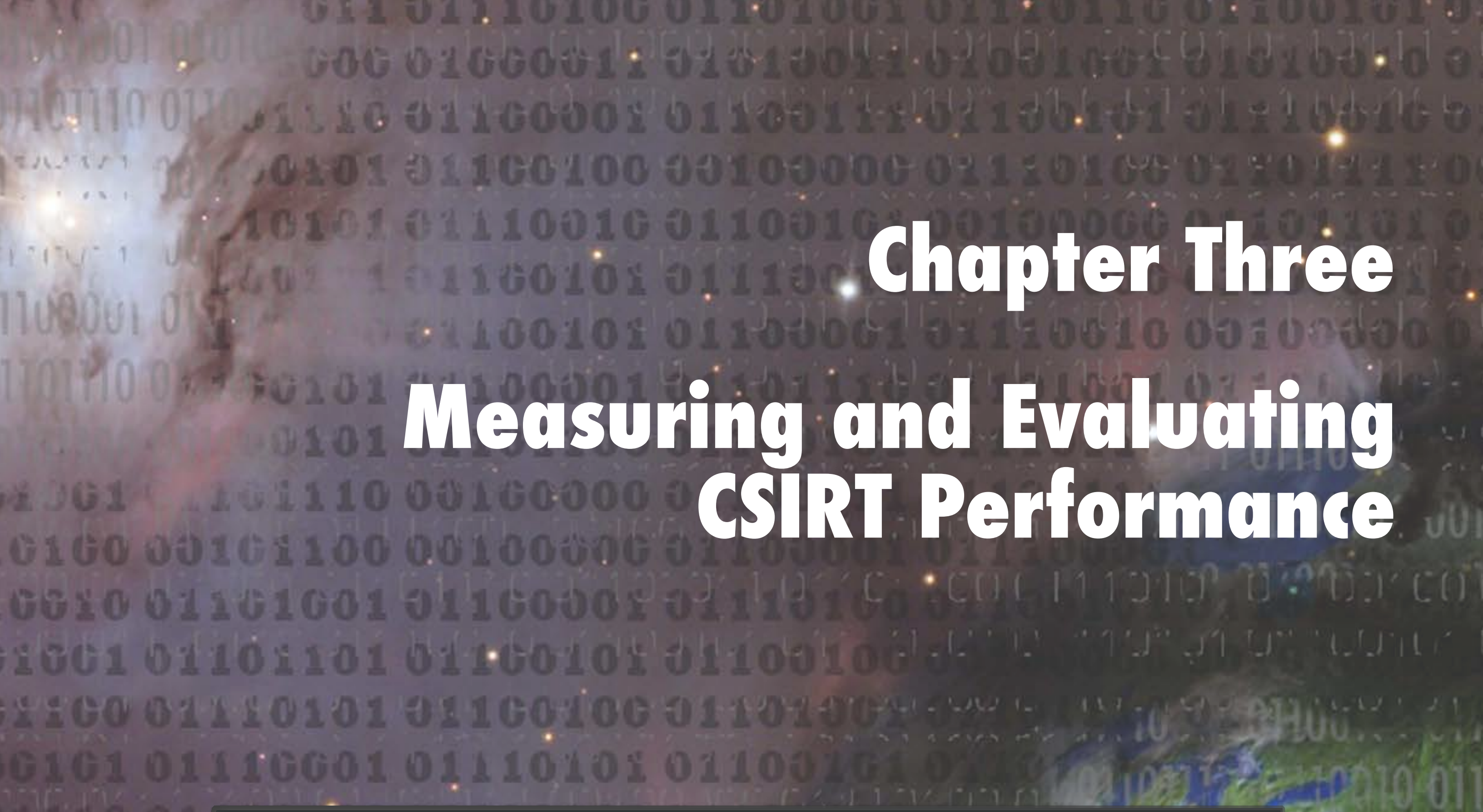
Teams	1. Watch	2. Incident Res.	3. Malware	4. Forensics	5. Threat Intel.	6. Engineering
1. Watch						
2. Incident Response	2 3					
3. Malware Analysis	1 2	2 3				
4. Forensics	1 2	3 4	3 4			
5. Threat Intelligence	3 4	3 4	2 3	2 3		
6. Engineering	4 4	1 2	1 2	1 1	2 2	
7 Communications	1 1	2 3	2 3	2 3	2 3	2 2

Routine incidents

Severe incidents

Key: Interaction levels

1. ***Little or no interactions:*** Teams generally work separately
2. ***Moderate levels of interaction:*** One team passes work to the next team
3. ***High levels of interaction:*** Teams pass work back and forth until incident is resolved
4. ***Very high levels of interaction:*** Teams work closely together, often gathering and meeting in the same space.



Chapter Three

Measuring and Evaluating CSIRT Performance

Key Themes

- Cybersecurity Incident Response Team (CSIRT) managers can use this chapter to determine how to measure CSIRT performance in a comprehensive manner.
- Comprehensive performance measurement enables CSIRT managers to identify strengths and areas for improvement in the way their CSIRTs function. It also enables CSIRT managers to make better-informed decisions about employee development decisions (e.g., training- or performance-related feedback) and personnel decisions (e.g., hiring, promotions, and, in some cases, firing).
- Performance should be measured directly rather than inferred through the use of maturity models.
- Performance metrics (or key performance indicators) are typically used to measure the efficiency, effectiveness, value, and impact of analysts' actions.
- CSIRT managers should use a set of metrics that (1) collectively capture the breadth of analyst performance, (2) are properly contextualized so as to avoid providing a misleading picture, and (3) do not measure factors extraneous to performance.
- Performance metrics should be supplemented by manager and/or client ratings of aspects of performance that cannot easily be measured objectively (e.g., performance quality). Moreover, comprehensive performance management requires the inclusion of additional outcomes (e.g., psychological outcomes such as well-being outcomes).
- Performance should be measured at the level of individual analysts, component teams, and the entire multiteam incident response system.
- Performance measurement can be summarized in a "balanced scorecard."

Contents

3.0 Introduction

Cybersecurity Incident Response Team (CSIRT) effectiveness depends upon how well individual analysts and the team as a whole perform various forms of work-related behavior that facilitate the CSIRT's priorities.

Although many CSIRTs measure CSIRT activity (e.g., number of incidents handled) or compare themselves to various standards (e.g., maturity models), the cybersecurity domain appears to lack a strategic, organized method of performance measurement and evaluation. This makes it difficult to properly determine cybersecurity effectiveness, as alluded to in the quotation from Jaquith on the next page. In this chapter, we discuss how to measure performance in a CSIRT context. Understanding how to measure performance is a necessary precursor to evaluating how well individual analysts and the overall CSIRT are performing.

Measuring employee job performance (let alone CSIRT performance) is a complex assignment because overall performance is the result of multiple types of behavior (Campbell, 1990). Therefore, the first step in employee performance measurement on any job is to conduct a job analysis. Job analysis helps to identify the tasks necessary to complete the job. The next step is to determine how to measure performance on each of these tasks. Once these initial steps are complete, managers can evaluate the extent to which each employee, and the team as a whole, performs well.

Many CSIRT managers use maturity models to evaluate (i.e., compare) the activities and processes of their CSIRTs to others. Maturity models provide much useful information about CSIRTs: for instance, they are used to document CSIRT activities and processes, business plans, client and customer needs, escalation plans, and official training policies (Stikvoort, 2015). Based on the information obtained from a maturity model, it is possible to make inferences about the performance of a CSIRT under the assumption that more mature CSIRTs perform better than less mature CSIRTs. However, these comparisons are founded upon inferences about performance (e.g., greater documentation of processes indicates greater performance). Rather than relying on such an indirect understanding of performance, direct performance measurement is more informative. The metrics (or key performance indicators) used should cover all the important tasks required to fulfill job responsibilities and should not cover any tasks not required to fulfill job responsibilities (i.e., tasks extraneous to the job). These aspects of performance measurement are not covered in maturity models.

In this chapter, we focus on the development of an effective performance measurement program that informs proper performance evaluation to determine CSIRT effectiveness. We address several issues that: (1) arise when measuring performance; and (2) cause sets of typically used metrics and ratings to be incomplete for, or irrelevant to, the job. We tie these issues to an assessment exercise that helps CSIRT managers determine whether they correctly measure performance in their CSIRTs. We also provide a set of broad categories of performance metrics and ratings that should prove useful for CSIRT managers. Finally, we provide strategies to guide the design of a comprehensive performance measurement program by addressing issues of completeness and including metrics from multiple areas of performance. In Addendum 1, we provide a table with various examples of published cybersecurity materials (e.g., government reports) that specifically discuss objectively-derived metrics.

3.1 Assessing Performance Measurement

The following assessment exercise is designed to provide managers with a diagnostic tool in order to determine how well performance is being measured and evaluated within the CSIRT. Based on the responses to this assessment exercise, managers can determine whether they would benefit from the strategies offered in this chapter. Managers should consider the time and resources required to implement these strategies relative to their need for improvement.

Assess how your CSIRT is functioning in this area by responding to the following statements on a 1-5 scale where 1= Strongly Disagree, 2= Disagree, 3= Neither Agree nor Disagree, 4= Agree, 5= Strongly Agree.

GO TO PAGE 70 FOR
STRATEGIES FOR CSIRT MANAGERS

ASSESSMENT EXERCISE

1. I consider not only conventional, objectively-derived performance metrics, but also subjectively-derived (e.g., using ratings) performance metrics.
2. I consider not only the quantity of performance, but also the quality of performance.
3. I consider not only how well an analyst performs under normal operating circumstances (i.e., "typical" performance), but also how he or she performs when confronted with very serious incidents (i.e., "maximum" performance).
4. I consider not only performance after an incident is detected (i.e., reactive performance), but also performance that occurs before an incident is detected (i.e., proactive performance).
5. I consider not only performance at the individual level, but also performance at the team level or other levels (performance at the broader multiteam system level).
6. I consider not only conventional performance outcomes, but also psychological (e.g., well-being) outcomes.

> **Security is one of the few areas of management that does not possess a well-understood canon of techniques for measurement. In logistics, for example, metrics such as 'freight cost per mile' and 'inventory warehouse returns' help operators understand how efficiently trucking fleets and warehouses run. In finance, 'value at risk' techniques calculate the amount of money a firm could lose on a given day based on historical pricing volatilities. By contrast, security has…exactly nothing. No consensus on key indicators for security exists.**
>
> **~ (Jaquith, 2007, p. xxi)**

3.2 Background

3.2.1 WHY IS A COMPREHENSIVE APPROACH TO PERFORMANCE METRICS IMPORTANT FOR CSIRTS?

Our interviews with CSIRT analysts and team managers demonstrated that CSIRT performance is measured in many ways; yet, agreement on what should be measured is limited. Performance measurement is important because of the old adage: "What gets measured gets done." To determine whether a CSIRT performs effectively, managers must be aware that a collection of metrics is needed, that not all metrics capture meaningful information, and that metrics can, at times, be misleading. Many individual metrics can be "gamed," and so our goal in this chapter is to provide managers with guidance aimed at generating a *set* of metrics and ratings that is collectively much more difficult to "game." Our suggestions in this chapter are guided by research on performance measurement and evaluation conducted by organizational psychologists, including research conducted in military settings (e.g., Campbell, 1990).

3.2.2 ISSUES WITH MEASUREMENT OF PERFORMANCE

A proper performance measurement and evaluation program requires that the manner in which performance is measured (e.g., via metrics) adequately captures the breadth of behavior required to perform well on the job in question. One common issue identified through our research was that CSIRT performance was often measured improperly, by inadvertent omission of important performance aspects (i.e., measurement deficiency) and inadvertent inclusion of aspects irrelevant to performance (i.e., measurement contamination). This issue is by no means unique to CSIRTs; rather, the organizational psychology research literature suggests that it is a typical phenomenon, across job types, in performance measurement.

Errors of Omission (Measurement Deficiency)

Many sets of performance metrics provided to us by CSIRT managers focused on some aspects of an analyst's job (e.g., incident handling and ticketing) but neglected other aspects of the job (e.g., communicating with end users). In other words, performance measurement and evaluation programs frequently capture only a portion of the analyst's job performance rather than the entire job. There is also a tendency to only measure performance in areas where objective performance is easy to determine. Organizational psychologists refer to such errors of omission as deficiency. As alluded to in the quotation below, measurement *deficiency* in CSIRT performance metrics leads to vulnerability.

Any single metric is almost certain to be a deficient measure of performance. We have developed a taxonomy of performance behavior and outcome for CSIRTs that we include as an appendix to this Handbook (see Appendix A). Proper performance measurement requires not just multiple metrics, but also metrics from each of the categories that collectively define performance—for instance, each of the categories from our performance taxonomy.

Although any single metric is very likely to be deficient when viewed in isolation from other metrics, it can be even more deficient than usual if it is not properly contextualized. For example, the number of incidents an individual analyst resolves could be an important metric. However, without contextual information such as incident severity level and the total number of incidents encountered by the CSIRT, it is difficult to determine whether the analyst actually performed his or her job well. An analyst who knows that he or she will be evaluated based solely on the number of incidents handled could "game" the system by selecting only low-severity incidents that can be handled quickly.

> **Focusing on individual issues alone and not on security as a whole leaves environments vulnerable.**
>
> **~ (Rashid, 2015).**

Measuring quality versus quantity.

CSIRT managers do not need to decide whether to emphasize quantity *or* quality—obviously, both should be emphasized. For instance, it is important to close a large number of tickets but also to receive high quality ratings from clients. A common problem for many CSIRTs, however, is that quantity is easier to measure than quality, resulting in a tendency to overemphasize quantity over quality—and, therefore, a tendency toward deficient performance measurement. In a subsequent section of this chapter, we discuss how to measure performance quality.

Measuring maximum versus typical performance.

The vast majority of performance metrics we encountered in our research on CSIRTs refer to "typical" performance. Typical performance includes the actions carried out by analysts and teams on a day-to-day basis. CSIRT managers can use measurements of typical performance to understand how individuals perform under normal operating circumstances. Measurement of typical performance is important because it is necessary for CSIRT managers to understand how team members perform during routine situations.

> **'This quarter we blocked 200 Million Spam Emails'...but how many were *not* blocked?**
>
> **~ (Alien Vault, n.d.)**

> **This quarter we saw a rise in the number of viruses detected on our systems by 20%.**
>
> **~ (Alien Vault, n.d.)**
>
> **....but is this because there are more viruses or because we are doing a better job of detecting viruses?**

On occasion, however, CSIRTs also encounter more severe incidents that require team members to operate at the maximum level of their capabilities. CSIRT managers who only measure typical performance generate deficient performance measurements because they fail to assess how team members perform during extreme situations. Managers can—and should—assess maximum performance as performance when confronted with the most severe incidents. However, because of the comparative rarity of such incidents, it is useful to estimate maximum performance in other ways as well. Organizational psychologists consider performance on exercises (simulations) to reflect maximum performance because employees are typically highly motivated to exert maximum effort—and because the short period of time associated with these exercises permits maximum effort. In contrast, over longer periods of time, fatigue and boredom can develop, and attention might not be sustained at such a high level. To properly assess maximum performance, exercises should be designed to simulate infrequent, major challenges with which analysts have little previous experience.

Measuring proactive versus reactive performance.

Performance relative to specific incidents can be divided into two categories: performance that occurs before an incident is detected (proactive performance) and performance that occurs after an incident is detected (reactive performance).

Proactive performance consists of future-oriented actions taken to achieve effective organizational outcomes in *anticipation* of changes in the external environment (Griffin, Neal, & Parker, 2007). This type of performance can help reduce the frequency and severity of future incidents (ENISA, 2006). Reactive performance occurs in response to an incident or request. The primary goals in the reactive stage include handling incidents and mitigating damage (ENISA, 2006). Reactive performance has been referred to as the "core component of CSIRT work" (Carnegie Mellon University Software Engineering Institute, n.d.-b).

Table 3.1 includes one example each of proactive and reactive performance. These examples were provided by cybersecurity professionals during our research interviews. In the proactive example, an analyst first discusses information that should be gathered regarding a client's network. As the analyst implies, the purpose of gathering this information during normal activity is to establish knowledge of baseline activities so that future changes to these activities trigger alerts regarding possible attacks. In the reactive example, an analyst discusses triaging an incident, where the purpose is to identify incident severity in terms of the number of servers affected. Once an incident is detected, the CSIRT must take actions to establish incident characteristics (such as severity) so as to handle the incident in the most appropriate manner. By measuring performance only before or after an incident is detected, the deficiency in measurement prevents CSIRT managers from knowing both how preventive actions contribute to CSIRT performance and how analysts respond to incidents when they occur.

Measuring performance at different levels of analysis.

Although many tasks can be accomplished by an individual CSIRT member (e.g., researching a new software patch), many other tasks require collaboration among CSIRT members (e.g., handoffs, escalation) and between multiple teams in a CSIRT multiteam system (CSIRT MTS; e.g., the CSIRT providing memory captures to a forensics team). For these reasons, CSIRT managers should ask the question: "What forms of performance should be measured at the individual, team, and MTS levels, and how should they be measured?" The inclusion of performance measurement at any or all of these three levels depends on the nature of the CSIRT's tasks and the level at which the CSIRT manager needs to identify strengths and areas for improvement.

TABLE 3.1 EXAMPLES OF PROACTIVE AND REACTIVE PERFORMANCE (QUOTES FROM ANALYST INTERVIEWS)

PROACTIVE	REACTIVE
"Starting out, we need to know the network. We need to know…how it's laid out, what devices are out there. How are we moving data from Point A to Point B? How does a client get out to the internet? We need to know what is there and who's managing those different pieces so [that] when we see [an] anomaly, we can go back to them."	"…we'll find something on the network. I'll send information to them. And they'll pull an image for the…box that's online. And then they'll crosscheck the data for us as well."

Individual performance is defined as the value of an employee's actions to the organization over a given period (Motowidlo & Kell, 2013). Individual-level performance requires one analyst to complete the task (e.g., writing an advisory). Team performance is defined as "the sum of individual and team processes" (Salas, Rosen, & King, 2007, p. 382; Smith-Jentsch, Johnston, & Payne, 1998). Team processes include collaboration and cooperation between members of the team. Performance at the team level includes a collective effort among team members (e.g., teaching each other). MTS performance is defined as the sum of individual, within-team, and between-team processes. Between-team processes include collaboration and cooperation between two or more teams that share a goal and that are located within a larger MTS. Performance at the MTS level includes a collective effort among teams (e.g., information exchange between teams; see Chapter 2, "The Social Maturity of CSIRTs and Multiteam Systems") for more information on MTS). Table 3.2 includes examples of tasks at each level. These examples were provided by cybersecurity professionals during our research interviews. To avoid measurement deficiency, CSIRT managers should measure performance at all levels relevant to a particular task or incident. For example, as the table suggests, the effectiveness of cooperation and information exchange between the monitoring and response teams is an aspect of the performance of the entire multiteam system.

A separate level of performance to be considered is the organizational level. Organizational metrics focus on how actions influence organizational outcomes. During our interviews, we encountered both stand-alone CSIRTs that serve external clients and CSIRTs housed within organizations that serve clients internal to the organization. Although we did not hear about the organizational level of performance in our interviews with either type of CSIRT, we did encounter references to organizational performance in cybersecurity books and documents published online. For stand-alone CSIRTs, organizational-level performance metrics might be redundant with those at the team and MTS levels. For CSIRTs housed within larger organizations, however, we found unique metrics that senior executives such as Chief Information Security Officers should consider. Examples include: labor costs to analyze security breaches, reinstallation of software and data recovery, and the percentage of system components that undergo maintenance on schedule.

Errors of Commission (Measurement Contamination)

Previously, we argued for the use of sets of performance metrics rather than individual metrics. However, one potential problem with sets of metrics is that they might contain irrelevant performance metrics. Organizational psychologists refer to the measurement of irrelevant, or non-performance-related, elements of the job as contamination. Contamination, like deficiency, is an error in measurement, but it is an error of *commission* rather than an error of *omission*.

Another contamination threat stems from the use of subjectively-derived performance ratings—that is, ratings that require considerable human judgment (e.g., manager ratings of analyst behavior). Although, in general, it is desirable to complement objectively-derived metrics with subjectively-derived ratings in order to generate a comprehensive understanding of CSIRT performance, subjectively-derived ratings have important limitations. Performance ratings completed by a manager, for instance, might be contaminated by the quality of the relationship between the manager and his or her employee: when the quality of the relationship is good, the employee might receive higher scores regardless of actual performance.

To be clear, we do not imply that subjectively-derived ratings should not be used. Quite to the contrary, they are an important addition to conventional, objectively-derived metrics. For example, we advocate the use of subjective ratings for the measurement of performance quality, which can be hard to measure objectively. However, managers should be careful not to contaminate their ratings with non-performance-related information.

As mentioned previously, CSIRT managers should identify all the tasks on which performance should be measured. Once they have done so, however, managers face the issue of how task performance should be evaluated. In some cases, CSIRT performance measurement and evaluation requires going beyond thinking in terms of specific "tasks." It is to these issues that we turn next.

3.2.3 PERFORMANCE-RELATED OUTCOME CATEGORIES

CSIRT performance outcomes can be broken down into three major categories:

- Performance outcomes assessed using conventional, objectively-derived metrics;
- Performance outcomes assessed using subjectively-derived ratings; and

TABLE 3.2 EXAMPLES OF TASKS AT DIFFERENT LEVELS (QUOTES FROM ANALYST INTERVIEWS)

Individual Level	"Basically your manager kind of creates unique goals for you at the beginning of the year and then you have a mid-year review like "how far am I toward those goals." They can be different for everyone."
Team Level	"…we'll do what's called a peer review. So we'll have other members of the team look at that ticket and kind of just put our heads together and kind of figure out what's exactly maybe going on, and see if we can figure it out, whether that ticket can be closed or if it needs to be escalated…"
Multiteam System Level	"[The] monitoring and response [team] and [the] expertise and advice [team] are in the same room. So there's very close cooperation, it's information exchange."

- Psychological outcomes (e.g., those related to well-being) assessed using subjectively-derived ratings.

Although our interviews, as well as published industry materials, provide the greatest number of examples for objectively-derived metrics, the other two categories should be considered if the goal is to create a comprehensive set of performance measurements. Below, we provide examples and explanations of each category.

Performance Outcomes Assessed Using Conventional, Objectively-derived Metrics

Many performance outcomes are assessed using ostensibly objective metrics. These metrics are "objective" in the sense that they do not require a person (e.g., a manager) to make a subjective rating of employees' scores on the metrics. Human judgment is, however, required in the selection and interpretation of these metrics for performance measurement and evaluation—for instance, in selecting only metrics that are relevant to performance and in properly contextualizing metrics (see our previous discussion of these issues).

Objectively-derived performance metrics were by far the most prevalent in our interviews with CSIRT managers and their team members. Through the creation of our performance taxonomy (see Appendix A) we identified eight sub-categories (e.g., quantity, incident handling capability, vulnerability reduction) that are typically measured using objectively-derived metrics. For each of the eight sub-categories, we provide definitions and specific examples (when available) from our interviews with CSIRT analysts (see Addendum 3.1). By using metrics from multiple sub-categories, CSIRT managers can take a more comprehensive approach to performance measurement and evaluation.

It is important to consider characteristics of objectively-derived metrics when creating a comprehensive approach to performance measurement and evaluation. First, these metrics are almost exclusively assessed by CSIRT managers in typical performance situations, meaning that there is often little understanding of how well cybersecurity professionals perform during extreme conditions (i.e., maximum performance). For example, incident handling capability is probably different during daily attacks versus an advanced persistent threat. Second, some of the sub-category metrics are more focused on reactive performance (e.g., "Time needed for remediation activities") whereas others focus more on proactive performance (e.g., "Percentage of critical systems reviewed for compliance with controls"). Finally, some of the sub-category metrics focus on individual-(analyst-) level performance (e.g., "Number of viruses/spyware programs detected [by an analyst] in user files"), whereas others focus on the team or MTS level (e.g., "Amount of time needed to reconfigure a system following an attack") or the organizational level (e.g., organizational reputation). Hence, CSIRT managers must include a variety of metrics from these sub-categories to capture a comprehensive understanding of CSIRT performance.

Performance Outcomes Assessed Using Subjectively-derived Ratings [1]

In addition to performance outcomes assessed using objective metrics, some performance outcomes are more appropriately measured via subjective ratings (e.g., by managers or clients/customers), for instance, on a 1-5 scale. [2] Based on models of job performance in the organizational psychology research literature (e.g., Rotundo & Sackett, 2002), and supplemented by data from our interviews, the outcomes to be assessed by subjective ratings fall into three major categories:

- Organizational citizenship behavior
- Counterproductive work behavior
- Quality of performance

Organizational citizenship behavior includes any voluntary (i.e., not a required role/task or included in the formal job description) behavior that contributes to the overall functioning of the CSIRT (or the broader organization), although such behavior is likely not regarded as central to the job (and therefore is not included in a job analysis); nor are instances of organizational citizenship behavior typically captured by technology. For this reason, organizational citizenship behavior is best measured through ratings such as those by the CSIRT manager. Examples of organizational citizenship behavior include voluntarily helping a coworker on his or her tasks, helping to resolve conflicts between coworkers and volunteering for tasks that are not required (e.g., improving a process).

The second category, counterproductive work behavior, includes intentional acts meant to harm the CSIRT (or the broader organization). CSIRTs are particularly interested in a certain form of counterproductive work behavior known as insider threat, which refers to someone with access to organizational systems "put[ting] an organization's data, processes, or resources at risk" (Pfleeger, Predd, Hunker, & Bulford, 2010, p. 170). Examples of these behaviors include downloading confidential information for personal gain and attacking company networks (Predd, Pfleeger, Hunker, & Bulford, 2008; Sarkar, 2010). CSIRTs should, however, also be interested in other forms of counterproductive work behavior such as taking overly long breaks during a shift or verbally abusing a coworker.

Some forms of counterproductive work behavior can be assessed objectively by electronically monitoring employee behavior. For instance, employee email, chat, and social media communication can be monitored and subjected to in-depth text mining. However, such intrusive forms of monitoring are likely to yield unintended consequences due to perceived trust violations (e.g., employees might

[1] In this section, we focus on manager ratings of the performance of their employees. We also discuss client/customer ratings of employee performance. However, it is also possible to get ratings of employees from other sources including coworkers and the employees themselves (i.e., self-ratings). We briefly discuss the last of these categories in the subsequent section on psychological outcomes.

[2] In other words, both objective (metrics) and subjective (ratings) approaches to performance measurement are numerical (quantitative).

quit and paradoxically be *more* likely to take intellectual property with them when they leave an organization). In fact, the insider threat literature appears to have been quite slow to acknowledge legitimate concerns regarding employee privacy, the ethics of monitoring, and so forth (Greitzer, Kangas, Noonan, Brown, & Ferryman, 2013). The bottom line is that, although certain forms of monitoring (e.g., using insider-threat-focused honeypots, monitoring unusually large uploads and downloads) are likely to be considered acceptable by employees, many highly intrusive forms of monitoring are not.

Instead, to reduce deficiency in performance measurement, managers should supplement appropriate objective measurements with subjective ratings of counterproductive work behavior. Although some forms of counterproductive work behavior may be performed covertly, employees may not always succeed in concealing their behavior. Other forms of counterproductive work behavior—repeated lateness and absenteeism, verbal and physical aggression toward coworkers, and so forth—are less readily concealable. Therefore, manager ratings of such behavior are appropriate.

For both organizational citizenship behavior and counterproductive work behavior, we suggest that managers keep records of particularly noteworthy instances of behavior that they have observed directly or that have come to their attention in other ways (e.g., coworker complaints that can be verified). Because memory is fallible, managers should document instances of these behaviors as they occur. Performance evaluations could then be based on behavior aggregated over the period of evaluation. For example, if performance evaluations are conducted every month, managers could use the following rating scale to assess both organizational citizenship behavior and counterproductive work behavior: 1 = "Never in the past month," 2 = "Once or twice in the past month," 3 = "Weekly," 4 = "Daily," and 5 = "Several times a day."

Table 3.3 lists examples of behavior that managers could document. These forms of behavior differ in their detectability; however, managers should document them when they are detected.

The third category, quality of performance (the extent to which an employee's performance is comprehensive and innovative), can also be measured subjectively. As mentioned previously, it is often easier to generate objective metrics for performance quantity than for performance quality. Moreover, many performance quantity metrics really assess activity level. Activity is important, but it must be accompanied by quality.

For instance, consider CSIRT analysts' contributions to an internal knowledge database wiki. It is easy to construct objective metrics to assess quantity of performance (e.g., number of updates to the wiki). However, the quality of the analyst's performance in this area is probably best assessed by manager ratings of issues such as the number of errors made by the analyst and the insight displayed

TABLE 3.3 EXAMPLES OF ORGANIZATIONAL CITIZENSHIP BEHAVIOR AND COUNTERPRODUCTIVE WORK BEHAVIOR THAT MANAGERS SHOULD DOCUMENT

FORM OF EMPLOYEE PERFORMANCE	EXAMPLES OF EMPLOYEE BEHAVIORS MANAGERS SHOULD DOCUMENT
Organizational Citizenship Behavior [3], [4]	• Keeps up to date on organizational changes that may influence CSIRT functioning • Keeps up to date on changes within the cybersecurity industry that may influence CSIRT functioning • Volunteers for tasks that are not part of his or her job but that benefit the CSIRT • Makes carefully considered suggestions to improve CSIRT effectiveness • Helps other CSIRT analysts with their work
Counterproductive Work Behavior [5], [6], [7]	• Misuses or sabotages data, applications, operating systems, or networks—or advises others on how to do so • Lies to supervisors or coworkers to cover up mistakes • Without good reason, arrives late for or departs early from a shift, takes overly long breaks during a shift, focuses on non-task behavior during a shift (e.g., plays computer games), or is absent altogether for a shift • Appears to be impaired at work due to alcohol or drugs • Verbally or physically abuses another employee or a client (e.g., incivility, assault, sexual harassment) • Puts the organization's data, processes, or resources at risk

[3] Borman, W. C., & Motowidlo, S. J. (1997). Task performance and contextual performance: The meaning for personnel selection research. *Human Performance*, 10, 99-109.

[4] Podsakoff, P. M., MacKenzie, S. B., Moorman, R. H., & Fetter, R. (1990). Transformational leader behaviors and their effect on followers' trust in leader, satisfaction, and organizational citizenship behaviors. *Leadership Quarterly*, 1, 107-142.

[5] Gruys, M. L., & Sackett, P. R. (2003). Investigating the dimensionality of counterproductive work behavior. *International Journal of Selection and Assessment*, 11, 30–41.

[6] Pfleeger, S. L., Predd, J. B., Hunker, J., & Bulford, C. (2010). Insiders behaving badly: Addressing bad actors and their actions. *IEEE Transactions on Information Forensics and Security*, 5, 169–179.

[7] Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioral and organizational measures. *Information Security Technical Report*, 15, 112-133.

by the analyst. Managers could, for example, rate the quality of a random sample of analyst updates to a wiki during a particular time interval, using a scale ranging from 1 ("Very low quality") to 5 ("Very high quality"). Doing so would also allow the manager to detect the behavior of an analyst who tries to "game" the performance evaluation system by making a large number of short, low-quality updates to the wiki so as to boost his or her performance quantity score.

Similarly, when incidents directly involve clients, clients should *routinely* be asked to rate the quality of the team member's (or the entire CSIRT's) performance. Client ratings could be used to determine resolution of client-relevant incidents. For example, rather than closing tickets when the analysts handling the incidents believe that the incidents have been resolved, a CSIRT might close tickets only when clients provide satisfactory ratings of incident handling quality (or else when clients do not respond to the satisfaction survey within a reasonable period). Client ratings could also be used as a way of evaluating the performance quality of a team member or the entire CSIRT. Specifically, performance quality across a given time interval could be determined by aggregating across all client-relevant incidents during the identified time interval.

Psychological Outcomes Assessed Using Subjectively-derived Ratings

In addition to performance outcomes, there are outcomes related to the ways individuals think and feel—outcomes referred to as psychological outcomes. Psychological outcomes are most appropriately measured via analysts' self-ratings as opposed to through either objective means or manager ratings. To protect analyst confidentiality, these ratings should be visible to management only at the CSIRT level (i.e., aggregated--not the individual analyst level).

> **"You could see the quality of an analyst's response…what the incident is and…their assessment…this analyst really knows what they're talking about… a lot of guys probably wouldn't have seen, but this one analyst [was] able to dig that out."**
>
> **~CSIRT Manager**

Moreover, it is important to note that although these psychological outcomes do not directly reflect the performance of the CSIRT, they are typically causes or consequences of CSIRT performance—and, in any case, they are meaningful outcomes in their own right (Colquitt, Scott, & LePine, 2007; Evans & Dion, 1991; Judge, Thoresen, Bono, & Patton, 2001). Therefore, these outcomes are important to consider even though they are often neglected in most discussions of CSIRT metrics.

Through a review of organizational psychology research, we identified four sub-categories of psychological outcomes. These categories are also part of the "Outcomes" column in various sections of our performance taxonomy (see Appendix A). Below (Table 3.4), we provide definitions for each of the four sub-categories as well as sources from which managers can obtain surveys to measure these outcomes.

3.3 Strategies for Designing a More Complete Performance Measurement Program

In this section, we provide strategies CSIRT managers can use to improve performance measurement and evaluation of employee performance. CSIRT managers can select the performance measures most appropriate to their team's function. CSIRT managers must also take into account the feasibility and cost of gathering particular measures of performance from their CSIRTs.

3.3.1 STRATEGY 1: BALANCE MEASURING QUANTITY AND QUALITY

Because both quality and quantity are important to CSIRT performance, CSIRT managers can use their discretion to determine the balance needed when measuring the quality and quantity of job behaviors. Whereas quantity can be measured via objectively-derived metrics, quality often requires managerial and client ratings. Such ratings can provide additional meaning and context to objectively-derived ratings. For example, it is one thing to understand the number of incidents resolved, but it is another to understand how well the incidents were resolved (e.g., contained versus completely eradicated from the system). We recommend that client-relevant incidents routinely be accompanied by a brief client survey containing two questions: one question in which the client rates the quality of the analyst's (or overall CSIRT's) technical performance in resolving the incident, and the second question in which the client rates the quality of the analyst's (or overall CSIRT's) interpersonal performance (e.g., professional demeanor).

3.3.2 STRATEGY 2: MEASURE MAXIMUM PERFORMANCE IN ADDITION TO TYPICAL PERFORMANCE

Although performance measurement during everyday situations is important, so is measuring maximum performance. This is because, in addition to analysts' everyday performance, managers are interested in analysts' maximum capabilities. Maximum performance can be measured through performance on periodically scheduled exercises (simulations). These exercises should be designed to simulate infrequent, major challenges with which analysts have little previous experience.

3.3.3 STRATEGY 3: MEASURE BOTH PROACTIVE AND REACTIVE PERFORMANCE

Measuring proactive performance provides a baseline for how the CSIRT performs prior to any response as well as indicating how effectively the CSIRT carries out preventive measures. On the other hand, measuring reactive performance provides a comparison point to baseline measures and indicates how effectively the CSIRT responds to incidents. Most CSIRTs are concerned about reactive performance, and they might pay less attention to proactive performance even though every CSIRT manager to whom we spoke confirmed that an appreciable portion of CSIRT tasks involved proactive behavior. Managers should therefore supplement reactive performance metrics with proactive performance metrics.

3.3.4 STRATEGY 4: DETERMINE THE APPROPRIATE LEVEL OF MEASUREMENT

The specific levels of performance metrics CSIRT managers should emphasize depend on the purpose behind measuring performance. If a manager wants to identify the strongest and weakest individual members in a CSIRT, the individual analyst level is most appropriate. If a manager wants to identify strengths and weaknesses in teamwork, the team or multiteam system level is most appropriate. Performance measures at the organizational level are often more appropriate for reports to upper-level management (e.g., the "bottom line"). Ultimately, the inclusion of performance metrics at all appropriate levels provides a more complete approach to performance measurement that informs performance evaluation.

CSIRT managers should keep in mind that certain performance measures might only be appropriate for certain levels of analysis.

TABLE 3.4 PSYCHOLOGICAL OUTCOME CATEGORIES ASSESSED USING SELF-RATINGS

OUTCOME	DEFINITION	EXAMPLE SURVEY ITEMS
Well-Being Outcomes [8]	Job-related outcomes associated with a change in the well-being of CSIRT analysts—for instance, the amount of stress experienced by analysts.	"To what extent does each of the following words or phrases describe your job?" • Demanding • Pressured • Hectic • Many things stressful • Pushed
Affective Outcomes [9]	Job-related outcomes associated with a change in attitudes held by CSIRT members, especially commitment toward, trust in, and satisfaction with the CSIRT or the organization.	"To what extent does each of the following words or phrases describe your job?" • Pleasant • Ideal • Worthwhile • Better than most • Makes me content
Cognitive Outcomes [10]	Job-related outcomes associated with the acquisition of skills and knowledge by CSIRT members or the development of shared knowledge of unique expertise among CSIRT analysts.	For each of the following, rate how strongly you agree with the following statements: • Each team member has specialized knowledge of some aspect of our projects. • I have knowledge about an aspect of our projects that no other team member has. • I know which team members have expertise in specific areas.
Motivational Outcomes [11]	Job-related outcomes associated with a change in task-related confidence of a CSIRT member.	For each of the following questions, rate how confident you are under the following circumstances: • If you encounter a difficult virus, how confident are you that you would be able to mitigate the incident before it escalates to the next level of severity? • If you are in need of help in handling an incident, how willing would you be to ask a teammate for help?

[8] Example survey items taken from: Stanton, J. M., Balzer, W. K., Smith, P. C., Parra, L. F., & Ironson, G. (2001). A general measure of work stress: The Stress in General scale. *Educational and Psychological Measurement*, 61, 866-888.

[9] Example survey items taken from: Ironson, G. H., Smith, P. C., Brannick, M.T., Gibson, W. M., & Paul, K. B. (1989). Construction of a Job in General scale: A comparison of global, composite, and specific measures. *Journal of Applied Psychology*, 74, 193-200.

[10] Example survey items taken from: Zhang, Z. X., Hempel, P. S., Han, Y. L., & Tjosvold, D. (2007). Transactive memory system links work team characteristics and performance. *Journal of Applied Psychology*, 92, 1722-1730.

[11] Example survey items adapted from: Weitlauf, J. C., Cervone, D., Smith, R. E., & Wright, P. M. (2001). Domain-specific self-efficacy scale [Database record]. Retrieved from PsycTESTS. doi: http://dx.doi.org/10.1037/t16510-000.

Collaboration between members of the same team should be measured at the team level whereas collaboration across teams should be measured at the multiteam system level. It is important that CSIRT managers identify the appropriate levels of analysis when determining how to measure and evaluate performance.

3.3.5 STRATEGY 5: CREATE A BALANCED SCORECARD OF PERFORMANCE MEASUREMENT

A tool that can help CSIRT managers maintain a comprehensive approach to performance measurement is the "balanced scorecard" (Kaplan & Norton, 1992). The balanced scorecard acts as a dashboard for a fast, yet comprehensive, review of performance. It also suggests relationships between different categories of performance. This approach can guide performance evaluation by helping managers prioritize which areas are most crucial to understanding the performance of their teams.

In line with what we proposed in this chapter, CSIRT managers should include measures that assess maximum and typical performance, quality and quantity of performance, proactive and reactive performance, organizational citizenship behavior and counterproductive work behavior, and performance at all the relevant levels (individual, team, multiteam system, and, if desired, overall organization). The balanced scorecard, therefore, is our single overarching recommendation in this chapter. If developed well, it can encapsulate all our other recommendations.

Each CSIRT may prioritize certain areas of performance. For example, some CSIRTs mostly deal with clients from outside their own organization. For these CSIRTs, performance at the reactive, individual level might be an important focus. Other CSIRTs mostly coordinate various teams' actions during incident response. For these CSIRTs, incident handling capability at the reactive, multiteam system level might be an important focus. As yet another example, a CSIRT manager who has noticed that competition among individual analysts is harming the functioning of the CSIRT may decide to prioritize team-level performance metrics over individual-level metrics.

A template for a balanced scorecard, as it applies to CSIRTs, is provided in Addendum 3.2 of this chapter.

3.4 Chapter Summary

An effective performance measurement and evaluation program can greatly benefit CSIRTs by providing information on individual, team, and multiteam system behavior that reflect successful job performance. Job performance should be measured with a variety of metrics that avoid issues with deficiency and contamination. Performance metrics can then be used by CSIRT managers, in conjunction with subjectively-derived ratings of performance, to evaluate the performance of individual analysts and the overall CSIRT. CSIRT managers can use the assessment exercise provided near the beginning of this chapter to better understand CSIRT performance as well as to diagnose how well they are evaluating the performance of CSIRT analysts and the CSIRT as a whole.

References

Alien Vault (n.d.). *Developing ITIL-Mature Security Incident Response with SIEM* [PDF document]. Retrieved from https://www.alienvault.com/blog-content/2011/11/SIEM-for-ITIL-Incident-Response-Part-1.pdf

Campbell, J. P. (1990). Modeling the performance prediction problem in industrial and organizational psychology. In M. D. Dunnette & L. M. Hough (Eds.), *Handbook of industrial and organizational psychology* (pp. 687-732). Palo Alto, CA: Consulting Psychologists Press, Inc.

Carnegie Mellon University Software Engineering Institute (n.d.-b). *CSIRT services*. Retrieved from http://www.cert.org/incident-management/services.cfm?

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology, 92*, 909-927.

ENISA. (2006). *A step-by-step approach on how to set up a CSIRT* [PDF document]. Retrieved from https://www.enisa.europa.eu/acitvities/cert/support/guide

Evans, C. R., & Dion, K. L. (1991). Group cohesion and performance: A meta-analysis. *Small Group Research, 22*, 175-186.

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. R., & Ferryman, T. (2013). Psychosocial modeling of insider threat risk based on behavioral and word use analysis. *E-Service Journal, 9*, 106-138.

Griffin, M. A., Neal, A., & Parker, S. K. (2007). A new model of work role performance: Positive behavior in uncertain and interdependent contexts. *Academy of Management Journal, 50*, 327–347.

Jaquith, A. (2007). *Security metrics: Replacing fear, uncertainty, and doubt*. Reading, MA: Addison-Wesley.

Judge, T. A., Thoresen, C. J., Bono, J. E., & Patton, G. K. (2001). The job satisfaction–job performance relationship: A qualitative and quantitative review. *Psychological Bulletin, 127*, 376-407.

Kaplan, R. S., & Norton, D. P. (1992). The balanced scorecard: Measures that drive performance. *Harvard Business Review, 70*, 71-79.

Kjaerem, I. (2005). *Benchmarking CSIRT work processes* (Master's Thesis). Gjovik University College, Sweden.

Microsoft TechNet (n.d.). *Responding to IT Security Incidents*. Retrieved from https://technet.microsoft.com/en-us/library/cc700825.aspx#XSLTsection124121120120

Motowidlo, S. J. & Kell, H. J. (2013). Job performance. In I. B. Weiner (Series Ed.) and N. Schmitt & S. Highhouse (Vol. Eds.) *Handbook of psychology: Vol. 12: Industrial and organizational psychology* (2nd edn., pp. 82-103). Hoboken, NJ: John Wiley & Sons.

Pfleeger, S. L., Predd, J. B., Hunker, J., & Bulford, C. (2010). Insiders behaving badly: Addressing bad actors and their actions. *IEEE Transactions on Information Forensics and Security, 5*, 169-179.

Ponemon Institute (2014). *Cyber security incident response: Are we as prepared as we think?* [PDF document]. Retrieved from https://www.lancope.com/resources/industry-report/ponemon-institute-report-cyber-security-incident-response-are-we-prepared

Predd, J., Pfleeger, S. L., Hunker, J., & Bulford, C. (2008). Insiders behaving badly. *IEEE Security & Privacy, 6*, 66-70.

Rotundo, M., & Sackett, P. R. (2002). The relative importance of task, citizenship, and counterproductive performance to global ratings of job performance: A policy-capturing approach. *Journal of Applied Psychology, 87*, 66-80.

Salas, E., Rosen, M. A., & King, H. (2007). Managing teams managing crises: Principles of teamwork to improve patient safety in the emergency room and beyond. *Theoretical Issues in Ergonomics Science, 8*, 381-394.

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioral and organizational measures. *Information Security Technical Report, 15*, 112-133.

Smith-Jentsch, K. A., Johnston, J. H., Payne, S. C. (1998). In J. A. Cannon-Bowers & E. Salas (Eds.). *Making decisions under stress: Implications for individual and team training* (pp. 61-87). Washington, DC: American Psychological Association.

Stikvoort, D. (2015). *SIM3: Security incident management maturity model* [PDF document]. Retrieved from https://www.trusted-introducer.org/SIM3-Reference-Model.pdf

The Center for Internet Security (2010). *The CIS Security Metrics, v1.1.0* [PDF document]. Retrieved from http://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf

ADDENDUM 3.1

TABLE WITH DEFINITIONS, EXAMPLES, AND SOURCES FOR OBJECTIVELY-DERIVED METRICS

CATEGORY	DEFINITION	EXAMPLE QUOTATION	EXAMPLE METRICS [12]	SOURCES FOR EXAMPLES OF METRICS
Quantity	An amount (e.g., count, percentage) related to workload for incident handling.	"We handle approximately… hundreds [of incidents], because we also have some automatic tooling that handles incidents for us."	• Number of thwarted (vs. successful) attacks • Number of data privacy escalations • Number of viruses/ spyware programs detected in user files • Percentage of systems with monitored event and activity logs	http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm?cs_pgIsInLView=1#8; http://www.securityinfowatch.com/article/10840065/metrics-for-success-security-operations-control-center-metrics; CIS_Security_Metrics; Jaquith (2007)
Efficiency	The amount of time taken to address issues.	"…We can have the phishing sites offline within 15 minutes after reporting it to us in every part of the world if it's needed. Fifteen minutes is the shortest time, but it's always in a really short time."	• Amount of time needed to triage vulnerabilities • Average time to mitigate vulnerabilities • Average time needed to grant (or revoke) customer access to company systems	Lancope; http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm?cs_pgIsInLView=1#9; Kjærem, 2005; http://technet.microsoft.com/en-us/library/cc700825.aspx#XSLTsection124121120120; CIS Security_Metrics
Secure Configuration	The technical application and maintenance of security policies on systems, applications, and network devices.	"We're working on a program, security breaches…[are] our milestones in the program and four times a year we discuss those milestones."	• Percentage of system with no known severe vulnerabilities • Percentage of system with security accreditations/ certifications • Number of missing operating system patches on each system • Number of machines covered by antivirus/ antispyware software	CIS_Security_Metrics; Jaquith (2007)

[12] These example metrics are taken from the cybersecurity literature on metrics. We would remind the reader, however, of our earlier caution that some of these metrics must be accompanied by additional contextual information so as to reduce deficiency. For example, rather than the number of viruses/spyware programs detected in user files, arguably a better metric would involve the ratio of this number to the total number of user files (because the total number of user files is likely to change appreciably over time). As another example, rather than the number of machines covered by antivirus/antispyware software, arguably a better metric would involve the percentage of all machines covered by antivirus/antispyware software.

ADDENDUM 3.1 (CONTINUED)

TABLE WITH DEFINITIONS, EXAMPLES, AND SOURCES FOR OBJECTIVELY-DERIVED METRICS

CATEGORY	DEFINITION	EXAMPLE QUOTATION	EXAMPLE METRICS [12]	SOURCES FOR EXAMPLES OF METRICS
Incident Handling Capability	The ability to detect and react to multiple computer security incidents in a skilled manner.	"…We'll go through the number of tickets that were worked, number of incidents worked, number of samples we sent to Symantec, the number that came back, you know, bad, good. So those are…the best kind of metrics, I think, we have that are actually numbers."	• Amount of time needed to close open vulnerabilities • Percentage of unplanned downtime due to security incidents • Average time between failures • Number of incidents successfully resolved	http://technet.microsoft.com/en-us/library/cc700825.aspx#XSLTsection124121120120; Jaquith (2007)
Recovery Capability	The ability to return to a pre-incident state.	"[S]ince they did that damage based on that live response data that we collect on the host, we're able to forensically go back through that and figure out how they did these prior steps.And then working with the task force or the detect teams not only to detect them earlier on but also to get protections in place so they can't even do those further steps."	• Average time needed to recover from incident • Time needed for remediation activities • Amount of time needed to reconfigure a system following an attack	CIS_Security Metrics; Jaquith (2007)
Employee Turnover	The change in the motivation of an individual CSIRT member to leave his or her job for another job in the same organization or in a different organization. [13]	"We lost a couple of colleagues because we are going towards this 24/7 situation."	No examples from published materials	No examples from published materials
Organizational Reputation	The change in external (e.g., customer) perceptions of an organization's products, jobs, and strategies. [14]	"There's the media, they play a big role…There could be a lot of attention on IT security, cybersecurity if you will, and if organizations are doing it wrong, especially with client data, there will be a lot of attention on that."	No examples from published materials	http://technet.microsoft.com/en-us/library/cc700825.aspx#XSLTsection124121120120
Vulnerability Reduction	The identification and remediation of known bugs or weaknesses (e.g., missing patches) that could lead to a compromise [15].	No examples from interviews	• Vulnerability scanning coverage • Percentage of critical systems reviewed for compliance with controls • Percentage of media sanitized prior to disposal • Percentage of systems monitored for deviations against approved configurations	CIS Security Metrics

[13] Campion, M.A. (1991). Meaning and measurement of turnover: Comparison of alternative measures and recommendations for research. *Journal of Applied Psychology, 76*, 199-212. Jackofsky, E. F., & Peters, L. H. (1983). Job turnover versus company turnover: Reassessment of the March and Simon participation hypothesis. *Journal of Applied Psychology, 68*(3), 490-495.

[14] Fombrun, C., & Shanley, M. (1990).What's in a name? Reputation building and corporate strategy. *Academy of Management Journal, 33*, 233-258.

[15] Cain, C. I., & Couture, E. (2011). Establishing a Security Metrics Program. *GIAC Enterprises*, 1-27.

Instructions: The balanced scorecard below will provide you with a comprehensive overview of how well your CSIRT is performing. First, determine which aspects of CSIRT performance you wish to measure. Then, identify quantitative goals for effective performance of each behavior and enter those numbers in the second column from the left ("Performance Goal"). You can then include subsequent data pertaining to actual performance in the third column from the left ("Actual Performance") and, if applicable, performance during a training program in the column to the far right ("Training Performance").

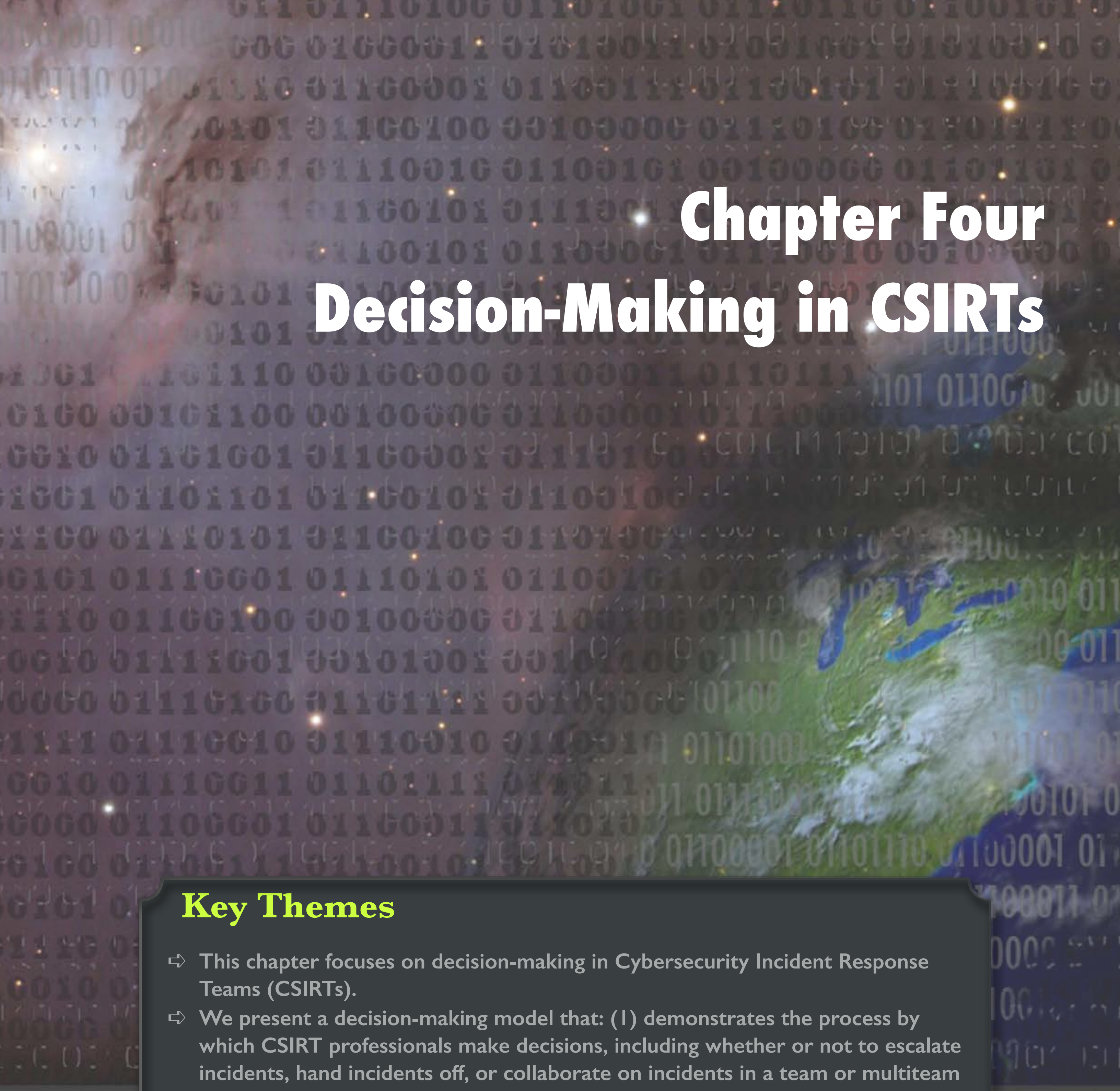
In the example below, for "Average time needed for analyst to proactively apply patch," the performance goal is 15 minutes, but the analyst exceeded that goal both on the job (12.5 minutes) and, to an even greater extent, during training (12 minutes). On the other hand, for "Average time needed for analyst to detect that an incident has occurred on the basis of an alert," the performance goal is 3 minutes and, although the analyst met the goal during training (3 minutes), his or her actual on-the-job performance fell short of the goal (4 minutes).

Note: The table below provides only a couple of examples to show how a balanced scorecard would work. A complete balanced scorecard would require the CSIRT manager to decide which forms of behavior he or she considers important components of CSIRT performance. Specifically, a complete balanced scorecard would include a variety of forms of behavior at the individual analyst, team, and multiteam system level. A complete balanced scorecard would also include behavior assessed by objective metrics (e.g., pertaining to performance quantity) but also behavior assessed by subjective ratings by CSIRT managers and/or clients (e.g., organizational citizenship behavior, counterproductive work behavior, and performance quality). For example, if managers use a 1-5 scale for their ratings (where 1 = "Never in the past month" and 5 = "Several times a day"), they could first set a goal of 3 ("Weekly") for organizational citizenship behavior and could then compare actual levels of on-the-job organizational citizenship behavior to that goal.

ADDENDUM 3.2

EXAMPLE OF A BALANCED SCORECARD FOR CSIRTS

BEHAVIOR (SELECTED EXAMPLES)	PERFORMANCE GOAL	ACTUAL PERFORMANCE	TRAINING PERFORMANCE (IF APPLICABLE)
Average time needed for analyst to proactively apply patch	15 minutes	12.5 minutes	12 minutes
Average time needed for analyst to detect that an incident has occurred on the basis of an alert	3 minutes	4 minutes	3 minutes
(etc.)			



Chapter Four
Decision-Making in CSIRTs

Key Themes

- This chapter focuses on decision-making in Cybersecurity Incident Response Teams (CSIRTs).
- We present a decision-making model that: (1) demonstrates the process by which CSIRT professionals make decisions, including whether or not to escalate incidents, hand incidents off, or collaborate on incidents in a team or multiteam system setting; (2) illustrates potential problems in decision-making; and (3) provides the basis for strategies aimed at addressing these problems.
- Strategies aimed at addressing decision-making problems in CSIRTs include various forms of training, cognitive prompts, and mnemonics.
- An adaptive case management (ACM) system provides a vehicle within which these strategies can effectively and efficiently be integrated.

Contents

4.0 Introduction

Cybersecurity Incident Response Teams (CSIRTs) are described throughout this handbook as teams with proactive and reactive functions—a distinction based on whether actions occur in preparation for or in response to a trigger. This chapter focuses on reactive functions, which characterize a majority of day-to-day tasks for cybersecurity professionals (West-Brown et al., 2003). Reactive functions begin with a response trigger. A trigger is a stimulus (such as an alert) that forces a cybersecurity analyst (or a team of analysts) to make one or more decisions. Within the cybersecurity context, an incident response trigger can be an indicator of a new incident.

For every incident response trigger, there is an initial decision regarding whether to tend to the event. If the choice is made to act (rather than, say, to immediately categorize the trigger as a false positive), there are numerous subsequent decisions that must be made (e.g., how much to prioritize that event over other events). The nature of the decisions following a response trigger varies according to the potential severity of the incident as well as the characteristics of the CSIRT (and its members) analyzing the trigger. The effectiveness of these decisions depends on the ability of the cybersecurity analysts to "collect and understand the right data at the right time in the right context" (Zimmerman, 2014, p.32). Common challenges to effective decision-making for cybersecurity professionals include overcoming biased decision-making and knowing when, how, and with whom to collaborate in responding to triggers.

This chapter begins with an assessment exercise to help CSIRT managers identify the strengths and weaknesses of their CSIRT's approach to incident response. Next, we present an evidence-based model of decision-making by professionals, modified to a cybersecurity incident response context--thereby demonstrating the decision-making process during incident response. We then discuss how decision-making in CSIRTs can go awry. We conclude this chapter with strategies to improve decision-making in CSIRTs.

4.1 Assessing Decision-Making Capacity

The following assessment exercise is designed to provide managers with a diagnostic tool in order to determine how well the CSIRT, individuals, or component teams within the CSIRT multiteam system (MTS) make decisions. This will ultimately help determine the social maturity of the CSIRT (See Chapter 2, "The Social Maturity of CSIRTs and Multiteam Systems," for additional information). Based on the responses to this assessment, managers can determine whether they would benefit from the strategies offered in this chapter. Managers should consider the time and resources required to implement these strategies relative to their need for improvement.

Assess how your CSIRT is functioning in this area by responding to the following assessment exercise on a 1-5 scale where 1= Strongly Disagree, 2= Disagree, 3= Neither Agree nor Disagree, 4= Agree, 5= Strongly Agree.

GO TO PAGE 83 FOR
STRATEGIES FOR CSIRT MANAGERS

4.2 Background

4.2.1 THE PSYCHOLOGICAL PROCESS OF INCIDENT RESPONSE DECISION-MAKING

The most accurate description thus far of how professionals make decisions under time pressure and stress is provided by the Recognition-Primed Decision (RPD) model. Klein and colleagues (Klein, 1989; Klein, Calderwood, & Clinton-Cirocco, 1986; Klein & Klinger, 1991; Lipshitz, 1993) developed this model after interviewing and observing

ASSESSMENT EXERCISE

1. Analyst expertise is considered explicitly when analysts are assigned (or assign themselves) to incidents.
2. Incident severity is considered explicitly when analysts are assigned (or assign themselves) to incidents.
3. Decision-making skills are emphasized in analyst training activities.
4. My analysts consider all necessary information before they make decisions in response to an incident.
5. My analysts comprehensively rehearse their response plans (including mentally testing them for ways in which they could go wrong) before implementing them.
6. When hiring new analysts, decision-making skills are emphasized.
7. My analysts decide correctly that they should include other analysts in their incident mitigation efforts.
8. Members on my team are proactive, soliciting help from team members.
9. My team solicits help proactively from other teams in the CSIRT multiteam system (MTS).
10. My team asks other teams in the CSIRT MTS to help them resolve an incident when such help is necessary.
11. My team takes the initiative when deciding to include other teams in a CSIRT MTS in their incident mitigation efforts.

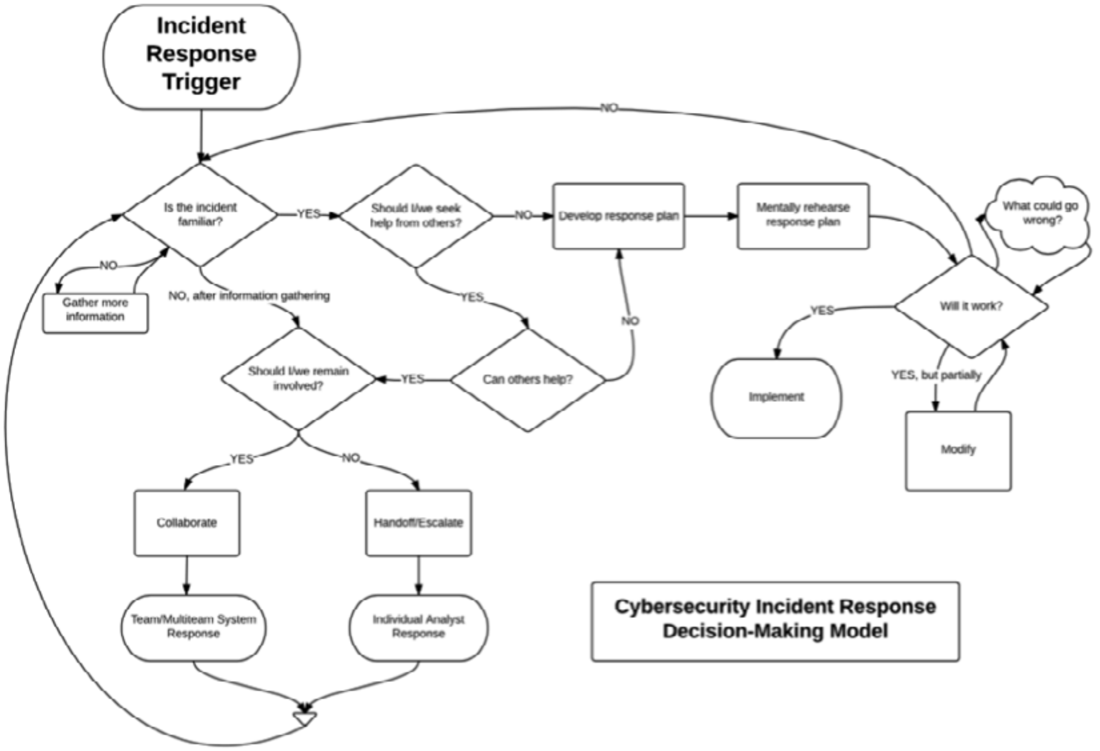

Incident Response Trigger
NO
Is the incident familiar?
YES
Should I/we seek help from others?
NO
Develop response plan
Mentally rehearse response plan
What could go wrong?
NO
Gather more information
NO, after information gathering
YES
NO
YES
Will it work?
Should I/we remain involved?
YES
Can others help?
Implement
YES, but partially
Modify
YES
NO
Collaborate
Handoff/Escalate
Team/Multiteam System Response
Individual Analyst Response
Cybersecurity Incident Response Decision-Making Model

Figure 4.1 Cybersecurity Incident Response Decision-Making Model

both experts and novices in several professions, including firefighters, tank platoon leaders, and design engineers. In this section, we describe a version of the RPD model that we have adapted to the cybersecurity incident response process. The model comes into play after an incident has been assigned to a particular analyst (or after an analyst has assigned an incident to himself or herself).

Figure 4.1 depicts the RPD model adapted to the cybersecurity incident response process.[1] The cybersecurity incident response decision process often starts with a low-level cybersecurity analyst opening a new ticket in response to a trigger (e.g., detecting a new event or receiving a new request from a helpdesk). The analyst first mentally classifies the incident as familiar or unfamiliar. As a part of this process, the analyst determines what information, currently missing, must be acquired to better decide whether the incident is familiar—and the analyst then focuses his or her efforts on acquiring that information. In some cases, the analyst may initially believe that the incident is familiar but may realize that this is not true and may need to return to the earlier stage of seeking out more information because the incident develops in unexpected ways.

If the incident is familiar and within the analyst's scope of ability, the analyst executes the response plan that worked well for similar incidents from the past. It should be noted that the analyst does not choose the best possible plan for the current incident. Indeed, according to the RPD model, the analyst does not actually compare all possible plans and so is not in a position to choose the best possible plan. Rather, having successfully matched the features of the current incident to similar incidents from the past that the analyst has resolved successfully, the analyst simply executes the response plan that worked for those past incidents.

If, on the other hand, the incident is unfamiliar--or if it is familiar but outside the analyst's scope of ability (e.g., based on incident severity)--the analyst must decide whether to involve other people--and, if so, whether to: (1) collaborate with other analysts in a team or MTS setting; [2] (2) handoff to other analysts who, despite being at the same level in the CSIRT hierarchy, possess greater expertise in handling this type of incident; [3] or (3) escalate to other analysts at one or more higher levels.

Yet, due to the nature of cybersecurity work, an incident may be unfamiliar to everyone in the CSIRT. Alternately, analysts to whom the incident is familiar may be unavailable to work on the incident. In such cases, according to the RPD model, the analyst(s) handling

[1] In addition to customizing the original model (Klein, 1989; Klein, Calderwood, & Clinton-Cirocco, 1986; Klein & Klinger, 1991; Lipshitz, 1993) to an incident response context, we customized it to account for the possibility that an analyst may escalate or hand the incident off to others or may work collaboratively with others (because the original process referred only to decision-making by an individual acting alone). We also obtained 49 cognitive task diagrams (involving the mental steps an analyst would take), associated with the analysis/triage and mitigation phases of incident response, from 25 CSIRT analysts. These cognitive task diagrams provided support for our modifications to the original RPD model.

[2] Team characteristics that influence the effectiveness of this collaborative incident response decision-making process (and strategies to improve upon them) are reviewed in Chapter 2 ("The Social Maturity of CSIRTs and Multiteam Systems"), Chapter 7 ("Collaborative Problem-Solving in Incident Response"), Chapter 8 ("Shared Knowledge of Unique Expertise"), and Chapter 9 ("Trust in Teams and Incident Response Multiteam Systems") of this handbook.

[3] Here, we refer to a handoff within a work shift to one or more analysts (or teams of analysts) with greater expertise in handling a particular type of incident. We do not refer here to a handoff necessitated by a change in work shifts.

the incident would develop a response plan and would then mentally rehearse “the successive steps to be taken, the potential outcomes of these steps, the problems that are likely to be encountered, and if and how these problems can be handled” (Lipshitz, 1993, p. 108-109). If a response plan seems likely to work, the decision-maker implements it. If, however, the response plan does not seem likely to work, the decision-maker once again cycles through the RPD process until he or she identifies a response plan that seems likely to work.

> “Usually if it's something I'm familiar with, then I'm usually comfortable with my own decision. I reach out to the group only when I have to or if it's new.”
>
> ~ CSIRT analyst

> “Well, today I'm working on something that--we're seeing alerts for certain traffic. And I'm trying to figure out, you know, why it's happening, whether we actually have a--something compromised on our network or whether it's something outside. I hit a dead end so I sent out an email to the whole team to see, you know, "Hey, can anyone else provide me any information? Have you seen this before?”
>
> ~ CSIRT analyst

> “Well, normally when we find artifacts, malicious or potentially malicious, we'll extract them and we will hand them over [to the] malware team for analysis.”
>
> ~ CSIRT analyst

> “Yeah, I mean the key...is also when to get leadership involved. That's a big decision about when to start escalating things. It's part of the process that we have in place of: I pass it to tier two, tier two will look at it. If this is going to go something bigger, then he'll get his management involved and it'll go up the chain. But you have to understand when that needs to happen.”
>
> ~ CSIRT analyst interviewed by us, discussing the escalation process

4.2.2 HOW DECISION-MAKING CAN GO AWRY

In CSIRTs, poor decision-making by analysts can lead to severe negative consequences for the organization as well as other entities such as clients and, in some cases, the public. The RPD model, importantly, also shows how decision-making can go awry. We now discuss three ways in which this can happen.

Expert Versus Novice Decision-Making

Research using the RPD model shows that novices (e.g., inexperienced analysts) not only make poorer decisions but also have more trouble with the decision-making process than do experts. Experts tend to move through the RPD process in one fluid process, with a very limited number of iterative loops. Experts' experience and knowledge allow them to recognize a situation, quickly select a response plan, mentally rehearse the plan, and implement the plan (Calderwood, Crandall, & Klein, 1987; Klein & Crandall, 1996).

Novices, on the other hand, require more time as they move through distinct phases of the process. Novices recognize situations less often because they have fewer points of reference from previous experience, and this lack of experience requires them to gather more information (Klein & Crandall, 1996). Once the information is gathered, novices are likely to have more difficulty than experts in choosing a good response plan. Novices are also likely to have more trouble at the mental rehearsal stage (e.g., O'Hare, Wiggins, Williams, & Wong, 1998). Finally, if a response needs to be modified slightly, novices are also likely to have trouble doing so. For example, a research study (Kobus, Proctor, & Holste, 2001) found that when operating under high uncertainty, although U.S. Marines with expertise in command-post management initially took more time than novice Marines to assess a dynamic tactical situation (on average, 15 minutes vs. 9 minutes), they then selected a course of action more quickly (on average, 4 minutes vs. 10 minutes) and also executed that course of action more quickly (on average, 8 minutes vs. 18 minutes).

The cybersecurity incident response context is similar to others that have been studied using the RPD model in the sense that cybersecurity professionals must quickly make decisions about ill-structured, high-risk problems that must be resolved under high time pressure and ever-changing conditions (e.g., Orasanu, 2005). An additional complexity associated with incident response (shared with only a few other types of jobs), however, is the uncertainty that exists about the intent of the adversary (Zimmerman, 2014). For these reasons, many decisions made by cybersecurity professionals could be viewed as critical decisions on which the security of a system relies.

Through 28 interviews with cybersecurity professionals, we gathered examples of critical decisions and asked the interviewees to explain how they reached their conclusions. Cybersecurity professionals also indicated the decision-making knowledge, skills, abilities, and other attributes (KSAOs) that were necessary for effectively handling cybersecurity events. The top three KSAOs (out of 18 discussed), along with definitions and percentages of interviewees who mentioned them, are provided in Table 4.1 above.

These three decision-making KSAOs all have strong ties to the RPD

TABLE 4.1 TOP THREE DECISION-MAKING KNOWLEDGE, SKILLS, ABILITIES, AND OTHER ATTRIBUTES (KSAOs)

KSAO (TOP 3 OF 18)	DEFINITION OF KSAO	% OF INTERVIEWEES MENTIONING KSAO (OUT OF 28)	EXAMPLE OF KSAO FROM INTERVIEWS
Problem Sensitivity	"The ability to tell when something is wrong or likely to go wrong" (Fleishman, Costanza, & Marshall-Mies, 1999, p. 179), and "it includes the specification of the problem as a whole as well as recognition of the elements of the problem" (Fleishman , Quantaince, & Broedling, 2008, p. 322).	96%	"First, take a look...at the actual traffic to determine whether or not it could possibly be anything malicious. Then the actual origin of it, determining, you know, is it some place safe or not, some place that's familiar or some place that's different."
Critical Thinking	The ability to "[use] logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems." (O*NET Online, n.d.)	93%	"After you do the remediation efforts, I would say that we go through a process then of deciding follow up.... Because some cases, depending on the type of remediation you do, you may just end it. I've handed it off to somebody else, I'm done. Or it may be something that I need to follow up on. Well, how bad was it? Do I need to follow up in 24 hours, 48 hours? Can I get back to them in a week? So you're already planning your next step in the process."
Information Ordering	"Ability to correctly follow a given rule or set of rules in order to arrange things or actions in a certain order" (Fleishman, Costanza, & Marshall-Mies, 1999, p. 179).	89%	"We followed the basic steps. We came in and, you know, what is the threat, what is the intrusion, what is the file? And then we want to know, you know, we want a copy of it. So while we're waiting on a copy of it, it's, well, how big is this? What steps can we take to find out how big this is, how widespread it is?"

model. Problem sensitivity, as defined in Table 4.1, is necessary for recognizing the elements of a problem, which is a precursor to determining whether an incident is familiar. Regardless of whether the next step involves gathering more information or using previously established rules to determine the scope of the incident, information must be organized or evaluated using information ordering skills. At a broader level, following a process to resolve an incident also requires information ordering skills. Finally, critical thinking skills are necessary during the mental rehearsal stage--for instance, when brainstorming what could go wrong if the preferred response plan were to be implemented.

These three KSAOs, moreover, help to illustrate expert-novice differences in decision-making. For example, with regard to problem sensitivity, novices are less adept at attending to the appropriate informational cues, and, thus, have lower sensitivity in detecting problems. As another example, with regard to information ordering, previous research has shown that experts are more effective than novices at applying general rules to specific situations (Randel, Pugh, & Reed, 1996).

Organizational psychologists have developed strategies that specifically target the development of decision-making KSAOs in novices. In the subsequent "Strategies" section of this chapter, we discuss how to strengthen these KSAOs through strategies such as structured troubleshooting training, critical thinking training, and developmental work assignments. Furthermore, we discuss how to select job applicants who already possess (and would bring with them to the job) high levels of these KSAOs.

Decision-Making Problems Affecting Both Experts and Novices

Unsurprisingly, experts generally make better decisions than novices. Experts moreover have less trouble with the decision-making process than novices. Expertise helps to reduce several forms of bias in decision-making (Cohen, 1993). However, expertise does not eliminate all forms of decision bias (Cohen, 1993). We focus on two areas where both experts and novices have problems.

First, experts are often overconfident about the accuracy of their decisions (Russo & Schoemaker, 1992). In other words, they think they make better decisions than they actually do. Second, experts are often predisposed toward seeking information that confirms their initial evaluation of a problem, known as confirmation bias.. As a result, they can miss important disconfirmatory information that would improve their decision accuracy (Heath, Larrick, & Klayman, 1998). But, of course, novices are by no means immune from overconfidence [4] and confirmation bias--these are general problems likely to affect most analysts, regardless of expertise. At a collective (team) level, biases such as overconfidence and confirmation bias can result in "groupthink," a phenomenon where the desire

[4] Novices are likely to be less confident than experts. But, as regards overconfidence, the issue is not how confident they are, *per se*, but rather whether their confidence exceeds their correctness.

for harmony in the team inhibits critical thinking and a willingness to disagree with the prevailing view. In the subsequent "Strategies" section of this chapter, we discuss strategies such as the five-why analysis and the premortem that can prevent overconfidence and confirmation bias in incident response decision-making.

The Role of Incident Severity

During the initial phases of the cybersecurity incident response decision-making process, cybersecurity analysts generally assess the severity of incoming incidents. Cybersecurity communities have developed various ways of assessing the severity of incidents. Generally, severity increases as a function of the trajectory of damage (e.g., increasing rapidly), the lifecycle stage at which the attack was discovered (e.g., the adversary has successfully obtained long-term system access versus the adversary has merely begun to investigate the target), the number of people who could be affected (e.g., clients, staff, the public), the status of the people who could be affected (e.g., the number of "Very Important People" affected), the potential financial impact to the organization and other entities (e.g., clients, the public), the potential informational impact (i.e., the "effect on the confidentiality, integrity, and availability of...information") to the organization and other entities, and the potential reputational impact to the organization (Cichonski, Millar, Grance, & Scarfone, 2012, p.3; see also Checklist Incident Priority, n.d.; Hutchins, Cloppert, & Amin, 2011; Johnson, 2014; Ruefle, Wyk, & Tosic, 2013).

Within a CSIRT, the severity of an incident typically dictates reporting--that is, the number and nature of people who must be informed and the promptness with which they must be informed. Incident severity also typically dictates incident response--for example, whether the analyst is expected to escalate the handling of the incident to a higher-level analyst. However, incident severity should also influence the manner in which analysts proceed through the RPD process. In particular, according to the RPD model, analysts mentally rehearse their preferred response plan, brainstorming things that could go wrong if the preferred plan were to be implemented.

> **"...we break those down into Severity 0, 1, 2, 3, and 4, Severity 0 being the highest criticality, Severity 4 being informational, password resets, those – so Severity 0, we probably get one of those every three months or so. Severity 1, which is it's still an intrusion into the network that's unauthorized, so we probably get maybe one or two of those a month."**
>
> **~ CSIRT analyst**

Yet, under some circumstances, decision makers may avoid extensive mental rehearsal and instead may focus on action (Klein & Klinger, 1991). Truncated mental rehearsal may occur, for example, if decision makers erroneously conclude that the incident is familiar to them. It may also occur when decision makers are under time pressure. Mental rehearsal, and especially an analysis of what could go wrong, is particularly important for high-severity incidents due to the higher cost of errors associated with such incidents. Moreover, mental rehearsal is more important for high-severity incidents than for high-frequency incidents because incident response in the latter case can be automated (albeit perhaps after a root-cause analysis, as as we discuss later) such that it does not require the analyst's attention at all. In the subsequent "Strategies" section of this chapter, we discuss a strategy (i.e., premortem) that is explicitly intended to enhance critical thinking regarding what may go wrong if the preferred plan were to be implemented. Crucially, because this strategy takes very little time to implement, it is useful even in situations involving high time pressure.

4.3 Strategies for Improved Decision-Making

In this section, we discuss how to select analysts who possess strong decision-making skills, how to train analysts to improve their decision-making skills, how to use cognitive prompts to reduce decision-making problems affecting both experts and novices, how to use mnemonics to capture the necessary information (e.g., for escalation or handoff), and how to use an Adaptive Case Management system as a vehicle for the incorporation of the training strategies, cognitive prompts, and mnemonics.

We note, in passing, that when cybersecurity professionals choose between handoff and escalation, they also decide to whom they should hand off or escalate the incident and what information about the incident they should disclose (Dalal, Bolunmez, Tomassetti, & Sheng, in press). These issues are largely beyond the scope of the current chapter, although the section on mnemonics touches on them indirectly. We refer the interested readers to Chapter 6 ("Information Sharing Effectiveness in Incident Response") of this handbook as well as extant research on handoff and escalation protocols (e.g., Alberts, Dorofee, Killcrece, Ruefle, & Zajicek, 2004; Daley, Millar, & Osorno, 2011).

4.3.1 STRATEGY 1: SELECTING FOR DECISION-MAKING SKILLS

When selecting applicants for CSIRT jobs, managers should attempt to assess the applicants' decision-making skills. The following sample questions are designed to assess an applicant's level of skill for problem sensitivity, critical thinking, and information ordering--that is, the top three decision-making-related skills in a CSIRT context. Please note that the situational interview questions below have not yet undergone a rigorous validation process (see Appendix C, "Hiring and Training CSIRT Employees: Validation Considerations"). They are, therefore, intended to provide CSIRT managers with an idea for the types of situational interview questions that can be used to measure an applicant's level of ability in problem sensitivity, critical thinking, and information ordering.

Problem Sensitivity

Question:

Describe a time when you recognized that an attack was about to take place. What information allowed you to recognize the impending attack? What details did you know about the problem from that information? What additional details did you want to find out about the problem?

ELEMENTS OF STRONG RESPONSES	RED FLAG RESPONSES
• Discusses a time when the attack was recognized before it affected the system	• Discusses a time when the attack was not recognized until long after it had affected the system
• Provides a detailed explanation regarding the information that indicated an impending attack	• Only provides a very surface-level explanation regarding the information that indicated an impending attack
• Expresses an understanding of the problem as a whole	• Does not express an understanding of the problem as a whole
• Expresses an understanding of the sub-elements of the problem	• Does not express an understanding of the sub-elements of the problem

Critical Thinking

Question:

Describe a time in which it was challenging to choose the approach for how you handled an event. Be as specific as possible in your description. What did you consider when choosing your approach? How did you justify using your chosen approach?

ELEMENTS OF STRONG RESPONSES	RED FLAG RESPONSES
• Discusses a time when choosing the approach for handling an event required thinking beyond repeating a previous choice or following a simple protocol	• Discusses a time when choosing the approach for handling an event only required repeating a previous choice or following a simple protocol
• Discusses the strengths and weaknesses of the approach used	• Only discusses the strengths of the approach used
• Discusses why other possible approaches were not chosen	• Does not discuss why other possible approaches were not chosen
• Provides logical, thoughtful rationale for the chosen approach	• Provides no rationale, or, at best, a surface-level rationale for the chosen approach

Information Ordering

Question:

Describe a time when you had to follow an established, multi-step process or protocol for gathering and organizing information about an event. Be as specific as possible in your description of the order in which you carried out the steps. What was the process or protocol you used? Why was it important to follow the process or protocol? How closely did you follow the process or protocol?

ELEMENTS OF STRONG RESPONSES	RED FLAG RESPONSES
• Discusses a very specific process or protocol that involves multiple steps	• Discusses a broad process or protocol that involves only one or two steps
• Provides a detailed explanation of the steps in the order in which they are designed to be carried out	• Provides a vague or disconnected explanation of the steps in the process
• Indicates an understanding of the rationale behind the process	• Is unable to articulate the rationale behind the process
• Indicates that he or she followed the process very closely--or else provides a compelling rationale for why he or she had to modify the process	• Indicates that he or she did not follow the process closely--and does not provide a compelling rationale for deviations from the process

Although situational interview questions do not have right or wrong answers per se, the strong responses and the red flag responses above should provide initial indicators in determining whether job applicants possess strong or weak decision-making skills.

4.3.2 STRATEGY 2: TRAINING DECISION-MAKING SKILLS

Structured Troubleshooting Training

One type of training that can help alleviate some of the weaknesses in novices' decision-making is known as structured troubleshooting (Schaafstal, Schraagen, & van Berl, 2000). This training is intended to increase how systematically novices approach problem-solving as well as to overcome the following issues novices experience when progressing through the RPD model:

- Unfamiliarity with the decision problem
- Need for extensive information search, possibly leading to information overload
- Inadequate knowledge of available response plans
- Need to organize thoughts regarding response plans into an ordered sequence of actions

Troubleshooting, or fixing issues in technical systems (Van Gog, Paas, & Van Merriënboer, 2006), is most effective when trainees are provided with "worked examples," or examples that include the following:

- A description of the problem
- Standards by which the adequacy of an end-state goal can be evaluated

- Process information: the steps that should be taken to reach the end-state goal

Structured troubleshooting, especially when worked examples are provided, therefore enhances the decision-making skills discussed previously. This, in turn, leads to better performance by cybersecurity analysts. A research study (Schraagen, 2009) that incorporated structured troubleshooting into an existing computer training course was able to decrease overall training time by 33% while yielding outcomes that were equivalent to those in the original training course in terms of knowledge (i.e., score on a knowledge test) and superior in terms of performance (i.e., solution quality, reasoning quality, and system understanding). Moreover, in contrast to more conventional troubleshooting training activities, which do not include either the necessary process information or the end-state goal standards, worked examples allow the trainee to focus on understanding the process, leading to further improvements in performance. Previous research has shown that trainees who undergo training with worked examples that include process information performed at least 60% better on the transfer of knowledge from the training to the job (even in job tasks with issues dissimilar to those in the training task) than those who did not receive worked examples (Van Gog et al., 2006).

Organizations interested in incorporating structured troubleshooting to their training programs should consider the associated development and implementation costs, which are mostly a factor of time investment. Development of the worked examples requires cognitive task analysis (CTA), a technique that involves prolonged interviews with cybersecurity professionals to examine "the knowledge, thought processes, and goal structures that underlie observable task performance" (Chipman, Schraagen, & Shalin, 2000, p.3). Once worked examples have been developed, instructors are trained to deliver this material to novice cybersecurity analysts. Thus, compared to the development of a traditional training program, the initial development of a structured troubleshooting program takes 8 times longer (i.e., 56 versus 7 days; Clark & Estes, 1996). Implementation time of a structured troubleshooting training, however, is about half of that of a traditional program. Specifically, as a result of the above-mentioned reduction in training time, both the time for delivery of the program by trainers (34 days versus 87 days to train a group of 500 novices) and the time that trainees need to take off from regular work activities (1 day versus 2 days per trainee; Clark & Estes, 1996) are much shorter. In sum, despite its high development costs, structured troubleshooting may be cost effective (due to its lower implementation costs) if large numbers of employees must be trained.

Critical Thinking Training

Critical thinking training focuses on improving the quality of decisions in unfamiliar situations under high time constraints (Cohen, Freeman, & Thompson, 1998; van den Bosch, Helsdingen, & de Beer, 2004). Recall that critical thinking was one of the "top three" decision-making skills reported by CSIRT analysts and managers.

For a CSIRT, critical thinking training would involve an experienced cybersecurity analyst guiding a novice (or group of novices) to create and evaluate a hypothetical cyber incident, come up with alternative interpretations of the situation, and make judgments about uncertainty and time pressure. While the novices engage in these steps, the expert analyst provides constructive feedback (e.g., "You should have prioritized opening that ticket") or asks clarifying questions (e.g., "Under what conditions would taking that computer offline be insufficient to address the problem?"). In addition, the expert analyst provides guidelines on when to think more deeply versus when to act quickly. Critical thinking training, therefore, optimizes the RPD process, especially the portion pertaining to the mental rehearsal of response plans.

Critical thinking training has been shown to improve the accuracy of trainees' assessments of a given situation. For example, in one study (Cohen et al., 1998), critical thinking training led trainees to consider 30% more causal factors, notice 58% more conflicting evidence, and generate 41% more alternative assessments.

As an alternative to critical thinking training, guided team self-correction (Smith-Jentsch, Cannon-Bowers, Tannenbaum, & Salas, 2008) can be used. This is a debriefing process conducted after training exercises. Prior to this process, expert cybersecurity professionals identify training scenarios (e.g., simulated incidents) and develop response plans for them. Following a training exercise, experts (who may or may not be the same as the experts who developed the training scenarios) facilitate a debriefing period featuring a review of the team's successes and failures in resolving the training incident.

The critical thinking training and guided team self-correction techniques are discussed in more detail in Appendix F of this Handbook ("Learning from Other Teams"). A part of that broader discussion emphasizes the costs associated with the initial development and subsequent implementation of these strategies. In summary, however, these strategies can have moderate to high development costs because they require an appreciable time commitment, not just from the experts who develop the training scenarios but also from the experts who must be trained to deliver the training. Implementation costs can be moderate because, in addition to typical training costs such as space and training equipment, the trainers and trainees must take time off from regular work activities for the training. Therefore, these techniques may not be as cost effective as some of the others described in this chapter.

Expert Modeling

Within a cybersecurity context, an expert modeling assignment requires that a novice analyst be paired with an expert on resolving an incident unfamiliar to the novice. For example, Hewlett-Packard uses an "L2 Assist" model that involves an expert (Level 2 analyst) being brought in to guide a novice (Level 1 analyst) through complex cases (Bhatt, Horne, Sundaramurthy, & Zomlot, in press). Alternately, a novice could be sent to work with an expert. Regardless, the novice analyst would be given the opportunity to propose a response plan. If the proposed plan is not adequate, the expert will provide constructive feedback regarding its shortcomings (DeRue & Wellman, 2009).

Expert modeling assignments incur costs because one person (either the novice or the expert, depending on who is sent to work with whom) must take time off from regular work activities, and because the expert may have to change his or her routine and devote more time to explanation in order to accommodate the training needs of the novice. However, compared to critical thinking training and guided team self-correction, expert modeling assignments are lower-cost activities because one of the two people (either the novice or the expert) does not have to spend time away from regular work activities. Moreover, the expert does not need to take the time to develop specialized training materials.

4.3.3 STRATEGY 3: COGNITIVE PROMPTS TO REDUCE OVERCONFIDENCE AND CONFIRMATION BIAS

Our previous strategies involved training aimed at improving skills, such as critical thinking skills, identified as the most important decision-making skills by CSIRT analysts and managers. That approach is targeted primarily at novice cybersecurity analysts. An alternative approach (though by no means mutually exclusive) involves the use of cognitive prompts associated with specific incidents experienced on the job. This approach is aimed at reducing overconfidence and confirmation bias and is targeted at both expert and novice decision makers.

We discuss two such strategies: "five-why analysis" and "premortem." These strategies, especially the premortem, are relatively simple and quick to execute and can, moreover, be targeted solely at the types of incidents (e.g., severe incidents) where they are most needed. They are, therefore, likely to be quite cost effective.

Five-Why Analysis

Five-why analysis (Ōno, 1988) is intended to eliminate conclusions that are plausible but not ultimately correct as well as conclusions that attribute blame to people (e.g., end-users) rather than the system (Heath et al., 1998). Originally developed at Toyota, the strategy is now widely used, including by Amazon.com's CEO Jeff Bezos (Serrat, 2009). Interestingly, one of the CSIRT analysts interviewed by us indicated that he uses the five-why analysis during incident mitigation.

The strategy involves decision makers asking five "Why?" questions to themselves so that they can arrive at the root cause of the situation. The strategy involves five questions (as opposed to, say, four or six) due to research suggesting that five questions are typically needed to locate a root cause. Importantly, each question must be answered through active investigation as opposed to off-the-cuff thinking. The incident response plan is then developed based on the answers generated in response to the root cause.

As an example of five-why analysis, consider a machine that has stopped working. Incident response might progress as follows (Imai, 1986, p. 50): 1. Why? "Because the fuse blew due to an overload." 2. Why? "Because the bearing lubrication was inadequate." 3. Why? "Because the lubrication pump was not functioning correctly." 4. Why? "Because the pump axle wore out." 5. Why? "Because sludge got in." As a result, the ultimate focus of incident response in this case involved attaching a strainer to the lubricating pump rather than a more intermediate countermeasure such as merely replacing the blown fuse. For another example of five-why analysis, in this case involving the failure of a production system due to the replacement of a single computer, see Olzak (2008).

The five-why strategy is widely acknowledged to be effective. In automotive assembly lines, five-why analysis created a 17% reduction in the time spent on ineffective performance strategies caused by insufficient analysis of the problem at hand (Wee & Wu, 2009). As another example, in a hospital where medical teams held daily 10-minute meetings to evaluate patients' conditions using five-why analysis (prior to developing patient treatment plans), the mortality rate was 61% lower, and major patient complications were 57% lower, than the regional rate (Culig et al., 2011).

It is important to note that five-why analysis is believed to be more effective for use by teams of cybersecurity analysts (in which members initially diagnose the problem independently) than by individual cybersecurity analysts. This is because when an individual decision maker has generated a seemingly compelling hypothesis, that hypothesis blocks his or her ability to generate alternative hypotheses (Heath et al., 1998). Five-why analysis, in other words, may not always be sufficient to overcome confirmation bias on the part of an individual decision maker (Heath et al., 1998). It is, however, a good candidate for use in situations when a cybersecurity analyst collaborates with other analysts in responding to an incident. In addition, the maximum value from the strategy is likely to be obtained when problems recur, such that a root cause must be found to eliminate further recurrences. Thus, the strategy may be of most use when a CSIRT notices that similar types of severe incidents recur over time.

Premortem

The second strategy, the premortem (Klein, 2007), is also intended to reduce overconfidence and confirmation bias. In a CSIRT context, a premortem would involve analysts being asked to imagine that they have already attempted to resolve the incident but that they have failed to do so successfully. The analysts would then identify reasons why the incident response effort may have failed. In other words, as opposed to a post-mortem (or an after-action review), which is carried out in hindsight, a premortem relies upon "prospective hindsight" to help analysts settle upon a good initial response plan and then further modify that plan so as to minimize weaknesses. The emphasis on identifying weaknesses rather than strengths in the initial response plan is deliberate in light of naturally occurring, overly optimistic thinking (i.e., overconfidence and confirmation biases).

The premortem strategy has been shown to be quite effective. For instance, a research study testing a similar strategy found a 12.8% decrease in decision bias (see Study 1 from Lord, Lepper, & Preston, 1984). Another study (Soll & Klayman, 2004) found that although decision makers who were 80% confident were normally correct only 30-40% of the time (indicating severe overconfidence), a decision strategy similar to the premortem led to decision-makers being correct almost 60% of the time (indicating milder overconfidence).

We, ourselves, have examined the usefulness of the premortem strategy in a CSIRT context via a simulated incident (involving abnormally high outbound traffic going to a server with a ".ru" domain). Prior to describing how they would resolve the incident, half the CSIRT analysts (randomly selected) were asked to perform a premortem--that is, to imagine that they had already responded to the incident and had failed--and to then provide reasons why they might have failed. The premortem strategy took very little time (typically 2-3 minutes). We found that, in general, analyst accuracy (as determined by expert analysis of analysts' response plans) and analyst confidence were negatively related. In other words, analysts who were less correct were actually more confident about their correctness. However, this was true to a much lesser extent for analysts who had completed the premortem than for analysts who had not. Completing the premortem led to an 8% increase in accuracy, accompanied by a 12% decrease in (excess) confidence.

As can be seen from these examples, the premortem can be quite effective when it is completed by an individual analyst. Moreover, similar strategies can be executed when a team of analysts collaborates on resolving an incident. For instance, one analyst can be assigned the role of "devil's advocate" (Schwenk, 1990). This analyst systematically critiques the team's preferred response plan, thereby exposing its weaknesses. Devil's advocacy, therefore, provides an effective antidote to "groupthink" by facilitating critical thinking and by providing a requirement to disagree with the prevailing view.

Both the premortem and five-why analysis can usefully be applied to high-severity incidents. If, however, a CSIRT manager needs to choose between them, the premortem might be preferable in most circumstances. This is because the premortem strategy is: (1) efficient, often requiring just a few minutes to execute (and is therefore more useful than five-why analysis in situations involving time pressure); (2) equally applicable to recurring and non-recurring incidents (whereas the five-why analysis is applicable primarily to recurring incidents); and (3) equally useful in individual and team decision-making settings (whereas the five-why analysis is more useful in team settings).

4.3.4 STRATEGY 4: USING MNEMONICS TO CAPTURE NECESSARY INFORMATION

Mnemonics facilitate the use of protocols that remind the decision maker to consider different aspects of a new situation (Heath et al., 1998). A widely used mnemonic in healthcare (as well as in nuclear submarines and the airline industry) is SBAR, which stands for Situation, Background, Assessment, and Recommendations (Riesenberg, Leitzsch, & Little, 2009). SBAR has been shown to improve the communication of patient information among healthcare staff in a number of studies and is reviewed in detail in Chapter 5 ("Communication Effectiveness During Incident Response") and in Appendix F ("Learning from Other Teams") of this handbook.

Following the success of SBAR, a number of other mnemonics have been developed in the healthcare industry to improve decision-making during patient diagnosis. One of these is SNAPPS: "Summarize history and [key] findings, Narrow the differential" (i.e., identify two or three alternative possible diagnoses), "Analyze the differential" (by comparing and contrasting the possible diagnoses), "Probe preceptor" (i.e., seek advice from a more knowledgeable person about uncertainties, difficulties, and different approaches), "Plan management" of patient care, and "Select case-related issues for self-study" (Wolpaw, Papp, & Bordage, 2009, p. 517). According to Wolpaw et al., senior medical students who used SNAPPS performed better than those who did not by making more than twice the number of diagnoses and justifying their diagnoses over five times more often. They also identified nearly eight times more uncertainties.

Of note, is that the SNAPPS mnemonic is relevant to the RPD model, in particular the portions of the model associated with developing and mentally rehearsing the response plan. Therefore, although mnemonics such as SBAR and SNAPPS would need to be modified for use in CSIRT work, the modifications should aim to retain, or even enhance, resemblance to people's actual (and ideal) decision-making processes. These modified mnemonics would be especially helpful if incorporated in CSIRT protocols for escalation, handoff, or even collaboration. The use of mnemonics within a team environment is discussed in Chapter 5 ("Communication Effectiveness During Incident Response") as well as in Appendix F ("Learning from Other Teams") of this handbook.

4.3.5 STRATEGY 5: USING ADAPTIVE CASE MANAGEMENT

In a CSIRT, analysts manually process incoming alerts generated by Security Information and Event Management (SIEM) software. Alerts that cannot be dismissed immediately are typically handled using case management systems that allow analysts to open "tickets" for and to track cases over their life-cycle (Bhatt et al., in press). Case management systems serve an important documentation function. However, a problem arises from the fact that traditional case management systems are designed on the basis of pre-specified workflow process models. Both the research literature on CSIRTs (e.g., Bhatt et al., in press) and our interviews with CSIRT analysts suggest that there is widespread dissatisfaction with these process models. Process models are viewed as either too general (and therefore unhelpful) or too specific (and therefore rigid) given the relatively unstructured nature of CSIRT work.

Adaptive case management (Hauder, Pigat, & Matthes, 2014), as applied to CSIRT work (Bhatt et al., in press), is an approach intended to address these concerns with process models—and to do so using an increasing focus on optimizing the use of available data. Adaptive case management (ACM) also integrates across tools and automates lower-level functions, thereby precluding the need for tedious cutting-and-pasting and, instead, freeing up analysts' time and cognitive resources for higher-level functions such as decision-making. In contrast to process models, an ACM system focuses on the individual case--that is, the incident. Rather than prescribing general processes the analyst is expected to follow, an ACM system provides context surrounding the incident by summarizing the ways in which similar incidents (based on formal incident classification systems) were handled in the past and the extent to which those previous remediation efforts were successful. Thus, an ACM system aims to guide the analyst and to provide the analyst with evidence-based (i.e., data-driven) suggestions but not to rigidly prescribe how he or she should handle incidents.

An ACM system provides a platform from which CSIRT managers can optimize recognition-primed decision-making by their analysts. Specifically, the RPD-based problems identified in this chapter, along with the strategies proposed to address them, can be addressed through the ACM system. We briefly discuss several examples.

First, the ACM system is explicitly intended to remedy expert-novice differences in knowledge, and, more generally, to provide all analysts with the information needed to successfully respond to incidents. This function is achieved by summarizing previous attempts at handling similar incidents.

Second, the ACM system can be used to teach novices decision-making skills. For example, the role of experts in expert modeling assignments (such as the aforementioned "L2 Assist" model) can, at least partially, be accomplished by the ACM system itself serving as the "expert." Other strategies, such as guided self-correction, can also be accomplished through the ACM system--in this case, by modifying the ACM system to require analysts to make decisions at each stage *before* seeing summary data (for similar incidents from the past) for that stage.

Third, the summary data provided by the ACM system can be designed to include information required by mnemonics such as the aforementioned SBAR and SNAPPS mnemonics. The use of these mnemonics would facilitate smoother escalations and handoffs. However, these mnemonics would be useful even in cases where a single analyst responds to an incident because the mnemonics would facilitate the initial choice of a response plan and its subsequent testing for weaknesses.

Fourth, cognitive prompts can be built into the ACM system. For high-severity incidents (as indicated by a formal incident classification system and/or by direct ratings of severity by the analyst), the ACM system could prompt an analyst to conduct a premortem. For high-severity incidents that have recurred (based on past summary data), the ACM system could prompt a root-cause analysis by a team of analysts through the five-why strategy.

Fifth, the ACM system could be used to assign specific incidents to individual analysts or teams of analysts. In so doing, the ACM system not only could derive insights from existing research on staff scheduling and rostering (see, e.g., Ernst, Jiang, Krishnamoorthy, & Sier, 2004), but also could address decision-making problems in several ways. Although, thus far, we have been discussing the data from previous instances of incident resolution as a way of guiding future incident resolution, these data could also be used to track individual analysts' experience with, and success in, handling specific types of incidents.

When such data are tracked, the ACM system can assign an incident to the analyst most qualified (of those currently available) to handle that incident. The ACM system can then also be used to optimize collaboration by assigning an incident to a team of analysts who, collectively, possess the knowledge needed to handle the incident. In other words, although it will probably remain important for CSIRT analysts to themselves mentally generate a Shared Knowledge of Unique Expertise (see Chapter 8, "Shared Knowledge of Unique Expertise"), such knowledge could readily be possessed (and disseminated) by the ACM system.

In addition to using assignment of incidents to analysts as a way to maximize performance, however, the ACM system could use assignment of incidents as a way to facilitate training. For instance, the ACM system could assign an incident to a combination of: (1) a novice analyst who *needs to acquire* the knowledge necessary to handle such incidents; and (2) an expert who is available to oversee the work of the novice. The ACM system could, moreover, emphasize training-based assignment of incidents (as opposed to performance-based assignment) only during periods of low incident volume--thereby minimizing the time costs associated with training. In summary, then, the ACM system could serve as a very useful vehicle for improving decision-making in CSIRTs.

4.4 Chapter Summary

This chapter focuses on improving decision-making in the context of the cybersecurity incident response process. We describe the psychological process of incident response decision-making, with an emphasis both on instances where analysts attempt to handle incidents themselves and instances where analysts either collaborate with others on incidents or else escalate or hand incidents off to others. We then discuss how incident response decision-making can go wrong and how it can be improved. We demonstrate how CSIRT managers can select job applicants who possess three important decision-making skills. We also suggest how these skills can be trained, and we discuss which training approaches are more versus less cost effective. We then suggest how incident response decision-making can be improved using simple cognitive prompts (such as the "premortem," which can be applied to high-severity incidents) and mnemonics that be incorporated into escalation and handoff protocols. Finally, we discuss an adaptive case management system and how virtually all the previously suggested strategies can efficiently be incorporated within such a system.

References

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). *Defining incident management processes for CSIRTs: A work in progress* (No. CMU/SEI-2004-TR-015). Carnegie-Mellon University, Pittsburgh, PA, Software Engineering Institute.

Bhatt, S. Horne, W., Sundaramurthy, S., & Zomlot, L. (2016). In S.J. Zaccaro et al., R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), *Psychosocial Dynamics of Cybersecurity (56-73)*. London, UK: Routledge.

Calderwood, R., Crandall, B. W., & Klein, G. A. (1987). Expert and novice fire ground command decisions. Alexandria, VA, USA: U.S. Army Research Institute for the Behavioral and Social Sciences. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a234877.pdf

Checklist Incident Priority. (n. d.). In IT Process Wiki. Retrieved from http://wiki.en.it-processmaps.com/index.php/Checklist_Incident_Priority

Chipman, S. F., Schraagen, J. M., & Shalin, V. L. (2000). Introduction to cognitive task analysis. In Schraagen, J. M., Susan F. C., & Shalin, V. L. (Eds). Cognitive task analysis. New York, NY: Psychology Press.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology Special Publication 800-61 Revision 2. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Clark, R. E., & Estes, F. (1996). Cognitive task analysis for training. *International Journal of Educational Research, 25*, 403-417.

Cohen, M. S. (1993). The naturalistic basis of decision biases. In G. A. Klein, J. Orasanu, & R. Calderwood (Eds.), *Decision making in action: Models and methods*. Norwood, NJ: Ablex Publishing.

Cohen, M.S., Freeman, J.T., & Thompson, B. (1998). Critical thinking skills in tactical decision making: a model and a training strategy. In J.A. Cannon-Bowers, & E. Salas Eds.). *Decision making under stress: implications for training and simulation*. Washington, DC: American Psychological Association.

Culig, M. H., Kunkle, R. F., Frndak, D. C., Grunden, N., Maher, T. D., & Magovern, G. J. (2011). Improving patient care in cardiac surgery using Toyota production system based methodology. *The Annals of Thoracic Surgery, 91*, 394-399.

Dalal, R. S., Bolunmez, B., Tomassetti, A. J., & Sheng, Z. (2016). Escalation: An understudied team decision-making structure. In S.J. Zaccaro et al., R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), *Psychosocial Dynamics of Cybersecurity*. New York: Routledge.

Daley, R., Millar, T., & Osorno, M. (2011, November). Operationalizing the coordinated incident handling model. In *Technologies for Homeland Security (HST), 2011 IEEE International Conference (pp. 287-294)*.

DeRue, D. S., & Wellman, N. (2009). Developing leaders via experience: the role of developmental challenge, learning orientation, and feedback availability. *Journal of Applied Psychology, 94*, 859-875.

Ernst, A. T., Jiang, H., Krishnamoorthy, M., & Sier, D. (2004). Staff scheduling and rostering: A review of applications, methods and models. *European Journal of Operational Research, 153*, 3-27.

Fleishman, E. A., Costanza, D. P., & Marshall-Mies, J. (1999). Abilities. In N. G. Peterson, M. D. Mumford, W. C. Borman, P. R. Jeanneret, & E. A. Fleishman (Eds.), *An occupational information system for the 21st century: The development of O*NET* (pp. 175–195). Washington, DC: American Psychological Association.

Fleishman, E. A., Quaintance, M. K., & Broedling, L. A. (2008). *Taxonomies of human performance*. Bethesda, MD: Management Research Institute.

Hauder, M., Pigat, S., & Matthes, F. (2014, September). Research challenges in adaptive case management: A literature review. In *Enterprise Distributed Object Computing Conference Workshops and Demonstrations (EDOCW), 2014 IEEE 18th International* (pp. 98-107). IEEE.

Heath, C., Larrick, R. P., & Klayman, J. (1998). Cognitive repairs: How organizational practices can compensate for individual shortcomings. *Research in Organizational Behavior, 20*, 1-37.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research, 1*, 80-106.

Imai, M. (1986). *Kaizen: The key to Japan's competitive success*. New York: McGraw-Hill.

Johnson, L. (2014). *Computer incident response and forensics team management: Conducting a successful incident response*. Waltham, MA: Elsevier.

Klein, G. (2007). Performing a project premortem. *Harvard Business Review, 85*, 18-19.

Klein, G. A. (1989). Recognition-primed decisions. In W. B. Rouse (Ed.), *Advances in man-machine system research* (Vol. 5, pp. 47-92). Greenwich, CT: JAI Press.

Klein, G. A., Calderwood, R., & Clinton-Cirocco, A. (1986). Rapid decision-making on the fire ground. *Proceedings of the Human Factors Society 30th Annual Meeting, 1*, 576-580.

Klein, G., & Crandall, B. (1996). *Recognition-primed decision strategies*. Alexandria, VA, USA: U.S. Army Research Institute for the Behavioral and Social Sciences. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a226887.pdf

Klein, G. & Klinger, D. (1991) *Naturalistic decision making; Human systems*. IAC Gateway, Vol XI No 3. Retrieved from http://www.au.af.mil/au/awc/awcgate/decision/nat-dm.pdf

Kobus, D. A., Proctor, S., & Holste, S. (2001). Effects of experience and uncertainty during dynamic decision making. *International Journal of Industrial Ergonomics, 28*, 275-290.

Lipshitz, R. (1993). Converging themes in the study of decision making in realistic settings. In G. A. Klein, J. Orasanu, & R. Calderwood (Eds.), *Decision making in action: Models and methods*. Norwood, NJ: Ablex Publishing.

Lord, C. G., Lepper, M. R., & Preston, E. (1984). Considering the opposite: a corrective strategy for social judgment. *Journal of Personality and Social Psychology, 47*, 1231-1243.

O'Hare, D., Wiggins, M., Williams, A., & Wong, W. (1998). Cognitive task analyses for decision centred design and training. *Ergonomics, 41*, 1698-1718.

Olzak, T. (2008). P*revent recurring problems with root cause analysis*. Retrieved from http://www.techrepublic.com/blog/it-security/prevent-recurring-problems-with-root-cause-analysis/

O*Net Online. (n.d.). Retrieved June 2, 2016, from https://www.

onetonline.org/find/descriptor/browse/Skills/2.A/

Ōno, T. (1988). *Toyota Production System: Beyond Large-Scale Production*. Cambridge, MA: Productivity Press.

Orasanu, J. (2005). Crew collaboration in space: A naturalistic decision-making perspective. *Aviation, Space, and Environmental Medicine, 76*(Supplement 1), B154-B163.

Randel, J. M., Pugh, H. L., & Reed, S. K. (1996). Differences in expert and novice situation awareness in naturalistic decision making. *International Journal of Human-Computer Studies, 45*, 579-597.

Riesenberg, L. A., Leitzsch, J., & Little, B. W. (2009). Systematic review of handoff mnemonics literature. *American Journal of Medical Quality, 24*, 196-204.

Ruefle R., van Wyk K., & Tosic, L. (2013). *New Zealand security incident management guide for computer security incident response teams (CSIRTs)*. New Zealand National Cyber Security Centre Government Communication Security Bureau. Developed in cooperation with the CERT® Division of the Software Engineering Institute at Carnegie Mellon University.

Russo, J. E., & Schoemaker, P. J. (1992). Managing overconfidence. *Sloan Management Review, 33*, 7-17.

Schaafstal, A., Schraagen, J. M., & van Berl, M. (2000). Cognitive task analysis and innovation of training: The case of structured troubleshooting. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 42*, 75-86.

Schraagen, J. M. (2009). Designing training for professionals based on subject matter experts and cognitive task analysis. In K. A. Ericsson (Ed.), *Development of professional expertise: Toward measurement of expert performance and design of optimal learning environments* (pp. 157-179). Cambridge, U.K.: Cambridge University Press.

Schwenk, C. R. (1990). Effects of devil's advocacy and dialectical inquiry on decision making: A meta-analysis. *Organizational Behavior and Human Decision Processes, 47*, 161-176.

Serrat O. (2009). *The five whys technique*. Washington, DC (USA): Asian Development Bank.

Smith-Jentsch, K. A., Cannon-Bowers, J. A., Tannenbaum, S. I., & Salas, E. (2008). Guided team self-correction impacts on team mental models, processes, and effectiveness. *Small Group Research, 39*, 303-327.

Soll, J. B., & Klayman, J. (2004). Overconfidence in interval estimates. *Journal of Experimental Psychology: Learning, Memory, and Cognition, 30*, 299-314.

Van den Bosch, K., Helsdingen, A. S., & de Beer, M. M. (2004). *Training critical thinking for tactical command*. TNO Human Factors Conference, Soesterberg, NL.

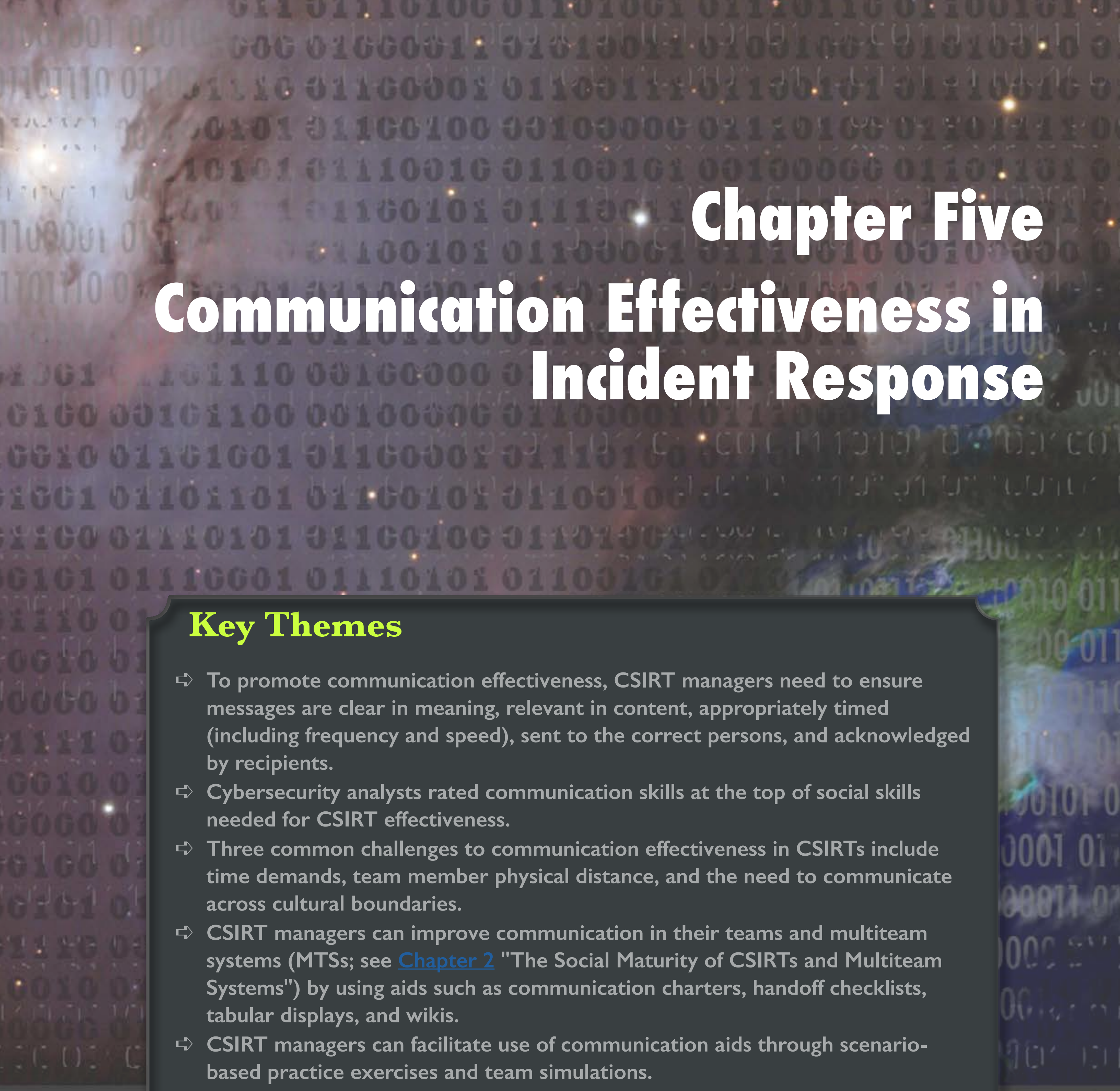
Van Gog, T., Paas, F., & van Merriënboer, J. J. (2006). Effects of process-oriented worked examples on troubleshooting transfer performance. *Learning and Instruction, 16*, 154-164.

Wee, H. M., & Wu, S. (2009). Lean supply chain and its effect on product cost and quality: a case study on Ford Motor Company. *Supply Chain Management: An International Journal, 14*, 335-341.

West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). *Handbook for computer security incident response teams (CSIRTs)* (No. CMU/SEI-2003-HB-002). Carnegie-Mellon University, Pittsburgh, PA. Software Engineering Institute.

Wolpaw, T., Papp, K. K., Bordage, G. (2009). Using SNAPPS to facilitate the expression of clinical reasoning and uncertainties: a randomized comparison group trial. *Academic Medicine, 84*, 517-524.

Zimmerman, C. (2014). Ten strategies of a world-cass cybersecurity operations center. Bedford, MA: MITRE Corporate Communications and Public Affairs.



Chapter Five

Communication Effectiveness in Incident Response

Key Themes

- To promote communication effectiveness, CSIRT managers need to ensure messages are clear in meaning, relevant in content, appropriately timed (including frequency and speed), sent to the correct persons, and acknowledged by recipients.
- Cybersecurity analysts rated communication skills at the top of social skills needed for CSIRT effectiveness.
- Three common challenges to communication effectiveness in CSIRTs include time demands, team member physical distance, and the need to communicate across cultural boundaries.
- CSIRT managers can improve communication in their teams and multiteam systems (MTSs; see Chapter 2 "The Social Maturity of CSIRTs and Multiteam Systems") by using aids such as communication charters, handoff checklists, tabular displays, and wikis.
- CSIRT managers can facilitate use of communication aids through scenario-based practice exercises and team simulations.
- CSIRT managers can enhance communication between teams by designating a specific person, for each component team, responsible for boundary spanning.
- Careful design of physical work spaces can facilitate more frequent communication, and sharing of information, with appropriate stakeholders.

Contents

5.0 Introduction

Effective communication is the cornerstone for information sharing and successful teamwork in CSIRTs (Aebersold, Tschannen, & Sculli, 2013). As shown in Figure 5.1, communication is the foundation of all the drivers of CSIRT effectiveness discussed in this Handbook.

The resolution of incidents or mitigation of potential threats begins with the communication of details to others. The purposes of cybersecurity communication are to:

- Provide situational awareness to key stakeholders;
- Exchange information about the tactics, techniques, and procedures of detected or potential threats as part of generating appropriate responses; and
- Transmit threat mitigation strategies.

Messages that are incomplete, untimely, or sent to the wrong people can delay cyber threat mitigation. Unclear or misinterpreted messages also hamper mitigation and resolution strategies. Indeed, the failure to communicate effectively with other CSIRTs, organizations, or industry sectors has negatively impacted several recent cyber attacks (e.g., the 2014 SONY cyber attack, Barrett & Yadron, 2015; the 2012 Deutsche Telekom cyber attack, Ministry of Security and Justice, the Netherlands; Federal Office for Information Security, Germany; Swedish Civil Contingencies Agency, Sweden, 2014). Despite the importance of communication, many CSIRT managers:

- Fail to pay significant attention to communication skills of applicants when selecting new CSIRT personnel for their teams;
- Do not use appropriate training protocols to develop communication skills in current personnel;
- Develop insufficient communication tactics and norms for their team(s); or
- Do not use or design work spaces to facilitate team and MTS communication.

In this chapter, we describe principles of effective communication sending and receiving. We also review three common barriers to effective communication in CSIRTs: time urgency, distribution of team membership (geographically, including across time zones, or across work shifts), and communication across different cultures. CSIRTs must also consider the relationship in place with the communication recipient. For example, internal communications may be less censored than communications a CSIRT is sending out to a peer organization or to the public at large; however, this chapter focuses on improving communication within a CSIRT. Specifically, this chapter covers the ways a CSIRT can overcome common communication barriers. We conclude the chapter with exercises and recommendations to improve incident response communication.

> **“Another thing is that the subjects that we work on, people are afraid. People do not want to share.”**
>
> **~ CSIRT member**

5.1 Assessing Communication Skills

A The following assessment exercise is designed to provide managers with a diagnostic tool in order to determine how well the CSIRT, individuals, and component teams within the CSIRT multiteam system (MTS) communicate. This will ultimately help determine the social maturity of the CSIRT (See Chapter 2, “The Social Maturity of CSIRTs and Multiteam Systems,” for additional information). Based on the responses to this assessment exercise, managers can determine whether they would benefit from the strategies offered in this chapter. Managers should consider the time and resources required to implement these strategies relative to their need for improvement.

Assess how your CSIRT is functioning in this area by responding to the following assessment exercise on a 1-5 scale where 1= Strongly Disagree, 2= Disagree, 3= Neither Agree nor Disagree, 4= Agree, 5= Strongly Agree.

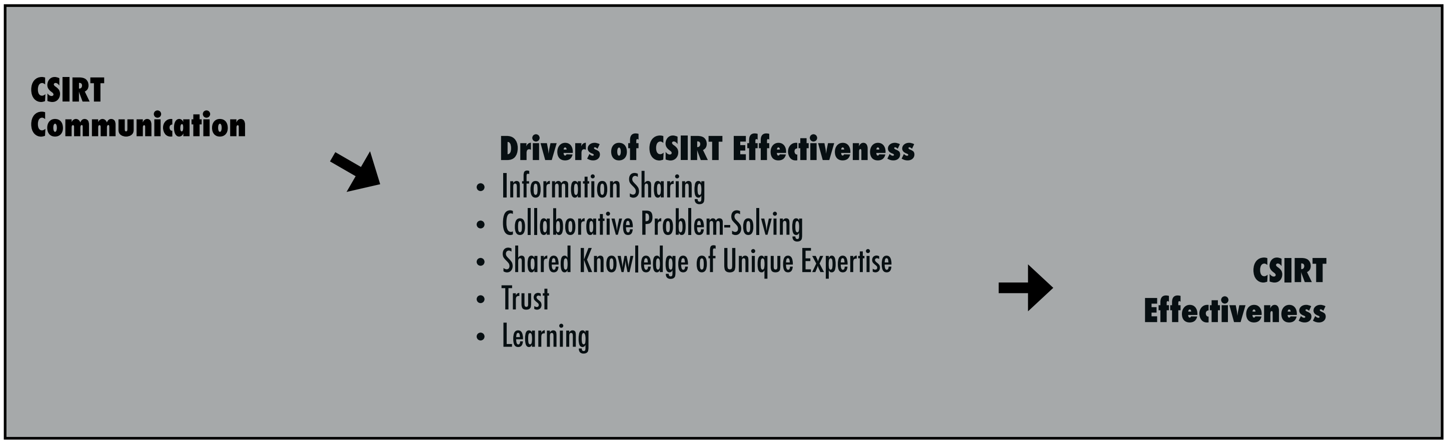

CSIRT Communication
Drivers of CSIRT Effectiveness
• Information Sharing
• Collaborative Problem-Solving
• Shared Knowledge of Unique Expertise
• Trust
• Learning
CSIRT Effectiveness

Figure 5.1 Communication as a Driver of CSIRT Effectiveness

ASSESSMENT EXERCISE

1. Messages sent among my team members contain all critical information.
2. Messages sent or received by the team are understood clearly.
3. My team members ask for clarification for messages received from others when they are unsure of something.
4. My team members confirm receipt and understanding of critical communications.
5. Information is received on time when trying to address a cyber threat.
6. Messages are sent to the correct recipient during different phases of incident resolution.
7. Complete and accurate information is passed during handoffs between different individuals in my team.
8. My team members quickly resolve communication issues with individuals on their teams.
9. My team members quickly resolve communication issues with team members from other cultures.
10. Messages sent between teams in the CSIRT MTS contain all critical information.
11. Different teams ask for clarification for messages received from other teams when they are unsure of something
12. Confirmation of receipt and understanding of critical communications occurs between teams.
13. Complete and accurate information is passed during handoffs between different teams.
14. Teams quickly resolve communication issues with other teams.
15. Teams in the CSIRT MTS designate a point person to communicate with other teams or external parties.

GO TO PAGE 99 FOR
STRATEGIES FOR CSIRT MANAGERS

5.2 Background Information and Project Findings

5.2.1 PRINCIPLES OF EFFECTIVE COMMUNICATION

Communication has two fundamental parts: the sending and receiving of messages (Hall, 1979; Riggio, 1986). The person *sending* the message must ensure that he or she communicates the right message to the right person at the right time using appropriate communication mechanisms. Persons *receiving* information must clearly acknowledge the message and follow up on anything that is not clear or understood. Cybersecurity work conditions often create difficulties for effective message sending and receiving. For example, cybersecurity professionals typically find themselves under immense pressure to communicate in both timely and effective ways during high impact threats. However, acting quickly can hurt the quality of communication. Important pieces of information might be overlooked, the message might be hard to interpret or not contain sufficient context, or some of the recipients who should receive information might get excluded inadvertently. The end result is slower, and potentially inadequate, incident response and resolution.

Researchers who recently developed a communications training program for military teams in mission-critical environments identified six principles of effective communication (Rench, Horn, Walker & Zaccaro, 2014, pp. 5-6). These six principles apply equally well to cybersecurity incident response communications. In Table 5.1, we pair each principle with a definition, an example of its occurrence in a CSIRT, and implications for any CSIRT that does not follow that principle.

> “I have seen teams not sharing 'everything they know' with other teams. They ask a question but tend to only share just enough to get whatever answer they are looking for. In return, they risk receiving an incomplete response to the detriment of incident resolution.”
>
> ~ CSIRT member

One of the communication issues that often affects many types of organizations, including CSIRTs, is the “failure to share unique information,” or the tendency to not communicate information or knowledge that only one team member might know. Team members are biased toward sharing knowledge that they all already have in common (Lam & Schaubroech, 2000; Stasser, Taylor & Hanna, 1989). Research shows that, typically, team members do

TABLE 5.1 PRINCIPLES OF COMMUNICATION IN INCIDENT RESPONSE

COMMUNICATION PRINCIPLE	DESCRIPTION	CSIRT EXAMPLE	CSIRT IMPLICATIONS
1. Relevance	Relevant communications include the most critical and appropriate information that pertains to problems faced by the team.	When CSIRTs work with one another to resolve an incident, sharing methods, findings, and new developments on a case is essential. The communicator must carefully consider the recipient and match the communication to the interest and needs of the audience.	During incident response, if one CSIRT MTS component team fails to provide relevant information to another CSIRT MTS component team, incident resolution might stall or remain incomplete. When sharing information about an incident with team members, the communicator must convey all of the critical details of the incident, while also not letting teammates get bogged down in the details.
2. Quality	High quality communications provide the necessary information for a problem. The information provided is accurate and error-free, and it is presented in a way that is easily understood by recipients.	Incident briefings or threat reports must be complete, accurate, and clear enough to enable others to act on the information. The content of an incident briefing must be carefully tailored to include all the relevant pieces of information.	Incomplete or inaccurate incident briefings or reports can result in less trust in findings and decreased likelihood that future information will be weighed seriously. Incident briefing content will vary depending on the incident and the needs of the CSIRT, but the specific content typically includes a description of the situation and its background, an assessment of what is needed, and recommendations on next steps for resolution (Hamilton, Gemeinhardt, Mancuso, Sahlin, & Ivy, 2006).
3. Timeliness	Timely communications provide information at the right time (i.e., neither too late nor too early) for team members to use in solving problems or making decisions.	Recipients of threat or vulnerability information need to receive information in time to prevent or mitigate intrusions.	If a CSIRT provides out-of-date threat information, bad actors have time to develop new methods, making the provided threat information meaningless.
4. Frequency	Communication frequency should be matched to the requirements of the situation, such that messages are sent often enough to maintain situational awareness, but not so often as to cause excess and distracting chatter.	Incident analysis updates should be provided so that appropriate situational awareness develops. Requests for such updates should not distract analysts from completing the necessary tasks to provide accurate updates.	Management or other stakeholders who request analysis updates too early (e.g., not enough time to complete the work) are likely to receive preliminary, incorrect or limited reports about the scope and severity of incidents.
5. Information Flow	Communication frequency should be matched to the requirements of the situation, such that messages are sent often enough to maintain situational awareness but not so often as to cause excess and distracting chatter.	If a team member has information from prior experience or knowledge that will help resolve an incident quickly and effectively, this information must reach those team members handling the incident in question.	When sending a message, senders should clearly determine the full range of analysts and stakeholders who need the information being provided. Failure to do so will mean that key analysts might lack the appropriate information needed to fully understand the incident.
6. Confirmation & Response	Recipients of communications should acknowledge receipt of critical messages; they should also follow up with senders when the meaning of the message content is unclear or not well understood.	After cyber threat information handoff, the receiving party should communicate that information was received and confirm they understand how to use the information.	If a CSIRT member receives specific, actionable threat information and does not respond appropriately to the sender of such information, senders cannot be certain that information was received or understood in the intended manner. Resulting miscommunications can slow down incident response.

Note: Adapted from Rench et al., (2014).

> **“Urgency is part of it. There’s always a great deal of pressure that you’re getting from a lot of different places. You’re getting a lot of questions really fast from a lot of people. You’ve got to be able to balance all of that.”**
>
> **~ CSIRT member**

not share knowledge that reflects their own unique expertise. For example, when discussing cyber threats, analysts will tend to talk with other analysts who share a similar understanding about the threat. Their conversations are more likely to confirm common information or perspectives rather than uncover new information. Cognitive scientists refer to this tendency in teamwork as the “confirmation bias” (Nickerson, 1998). Unless analysts are being encouraged by their managers or by established communication norms, one should not assume they will share their unique expertise, information, or insights. Communication failure caused by not sharing relevant information can result in costly errors and delays during critical incidents.

This failure to share unique information can be worse when information is being transmitted between different teams in an MTS. Members of teams naturally tend to communicate more frequently and send more information to their fellow team members than to members of other teams, especially when those other teams have very different work functions from their own team. Furthermore, our focus group interviews indicated that such inter-team communication in a CSIRT MTS needs to occur more frequently in severe or high impact incidents. Accordingly, the failure to share unique information between different teams can cause significant delay in resolving major incidents.

Communication Errors and Team Failure

The six communication principles described in Table 5.1 might appear straightforward; however, in many situations, team failures can be attributed to poor communication --defined by a failure to apply these six principles-- particularly in event and emergency response teams like CSIRTs.

Communication failures have been documented often in CSIRTs. A study where CSIRTs engaged in simulated communication exercises found that teams made critical communication mistakes such as sending information to the wrong recipients (principle 5, information flow), not responding in a timely manner to communication (principle 3, timeliness), and failing to provide requested information (principle 1, low message relevance; and principle 2, message quality; Tjaden & Floodeen, 2012). In the Deutsche Telekom AG attack in 2012, cyber attack mitigation was delayed because information related to identification of the lead organization responsible for response coordination was not known or provided when threat information was first shared (principle 3, timeliness; Ministry of Security and Justice, the Netherlands; Federal Office for Information Security, Germany; Swedish Civil Contingencies Agency, Sweden, 2014). Deutsche Telekom AG knew they had to quickly notify the Federal Criminal Police Office because the attack involved critical infrastructure (i.e., telecommunication and internet), so they communicated based on timeliness (principle 3). However, they should have considered sending a more informative message (principle 2, higher quality; and principle 1, relevance), or taking time for confirmation and response (principle 6), which could have prevented this delay.

The Deutsche Telekom AG attack example points to the challenge of communication for CSIRT managers − different communication principles might clash in the heat of responding to an urgent event. To meet this challenge, CSIRT managers need to develop and practice communication protocols within their teams-- a recommendation we return to later in this chapter (and in Chapter 6 - "Information Sharing Effectiveness in Incident Response"). CSIRT members should always try to apply *all* principles of effective communication. This can sometimes mean contributing what you do know up front, and seeking stronger/more information in a timely follow-up.

In summary, effective communication depends greatly on effectively sending and receiving information. It is vital that communicated messages be sent in clear, concise ways and contain the appropriate level of background information to understand the situation. Accordingly, a major responsibility for CSIRT managers is to develop procedures that help their teams understand when, how, to whom, and how frequently to communicate key information. Managers also need to be aware of certain barriers that often constrain communication effectiveness in CSIRTs. We cover three such barriers in the next section.

> **“If you’re managing global teams and working globally, the time zone difference is probably one of the biggest challenges.”**
>
> **~ CSIRT member**

Three Common Challenges to Effective CSIRT Communication

According to our focus group interviews with CSIRT members, we noted three challenges that can interfere with effective communication: time urgency, physical and temporal dispersion of team members, and cross-cultural differences. We describe these challenges below. We then provide recommendations CSIRT managers can use to overcome communication breakdowns in a later section.

Time Urgency

Cyber threats, particularly high impact incidents, often require very quick responses to mitigate damage. However, in teams similar to CSIRTs, time demands have been found to reduce the quality and frequency of messages (Gladstein & Reilly, 1985; Weick, 1990). CSIRT managers should develop protocols on how to

> **We get more from the local guys just because they're here and they know us. And we're in that same time zone. It’s easier to communicate with the local folks than [those geographically dispersed]. Because they're right here. Something comes up. A lot of times you literally walk over there and say, ‘What are you seeing?’**
>
> **~ CSIRT member**

communicate information under conditions of time urgency and practice them during training exercises until effective communication under time pressure becomes the norm (see section 5.3.1 below on team charters).

Team Dispersion

Although cybersecurity professionals might belong to the same CSIRT, they might not work together at the same time or in the same physical space. Instead, team members might be “temporally dispersed” (working at varying times, e.g., different shifts or time zones) and/or “geographically dispersed” (working in different physical locations). For example, some CSIRTs might function on a 24-7 basis, requiring geographic displacement of multiple shifts over various times of day. These kinds of dispersion are magnified at the MTS level, where different teams may work at different times and different physical locations.

Both kinds of dispersion, team and MTS, can impair communication. Geographically dispersed teams communicate less frequently than face-to-face teams (de Guinea, Webster, & Staples, 2012). When CSIRT leaders manage dispersed teams, they need to establish protocols that foster greater communication among dispersed subordinates while ensuring that communication is not dominated by a smaller number of team members. Communication plans established by CSIRT managers should focus on key elements of how information exchanges occur across the temporal and geographic CSIRT boundaries. In Section 5.2.2 of this chapter, we provide guidance on information checklists to assist with communication between shifts, across time zones, or across geographic regions.

The Impact of National Cultural Differences on Communication

Cultural differences within and across CSIRTs can pose significant communication challenges (Watson, Kumar, & Michaelson, 1993), partly because each culture has its own set of values, orientations, and priorities. Different cultural practices can lead to communication misunderstandings (Gibson & Vermeulen, 2003). For example, some cultures tend to avoid conflict during communication, while others are more accepting of debate and discussion (Berry, Carbaugh, Innreiter-Moser, Nurmikari, & Oetsch, 2009). Cross-cultural communication can lead to conflict when members view differing communication practices as uncomfortable, or even offensive.

Another fundamental cross-cultural communication issue that exists across all types of organizations is the tendency to communicate more openly with members of one’s own cultural group and less openly with members of other cultural groups (White & Whitener, 1998). Cultural identity can influence intergroup dynamics (Hambrick Davison, Snell, & Snow, 1998). Members of different cultures generally have different views about how and with whom information should be shared, potentially lowering the quality and relevance of messages sent across cultural boundaries.

Two important aspects of national culture, called “collectivism” and “power distance,” can influence communications between cybersecurity professionals from different countries. Members from collectivistic cultures usually identify more strongly with their group and tend to have more positive attitudes towards knowledge sharing within their group; members of less collectivistic (more individualistic) cultures generally share less information (Hwang & Kim, 2007). Such cultural differences can impair information flow when contrasting cultures attempt to communicate.

Similarly, power distance can influence information flow. Power distance refers to the extent to which a country emphasizes status differences and a hierarchical distribution of power (Hofstede, Hofstede, & Minkov 2010). People from countries that are higher in power distance usually demonstrate more formalized top-down flow of knowledge compared to people from countries low in power distance (Ford & Chan, 2003). High power distance countries usually have authoritative leadership, centralized decision structures, inequality between lower-- and higher-- level employees, and lower levels of trust (Hofstede, 1984). Information sharing in such contexts might only happen under higher-level managers’ instructions. Low power distance countries are more likely to develop participative leadership, decentralized decision structures, and higher levels of trust (Hofstede, 1984), enabling information sharing to naturally occur more readily in both directions. CSIRT managers who communicate with countries higher or lower in power distance should be aware of potential differential information transfer (flow) patterns.

> **Even in Europe, there’s a different working culture within countries. If you look at the Netherlands we have a real open culture. I mean I can swear at my boss and he won’t have a grudge. I mean that’s real typical Dutch. But if you go to Germany, for instance, that’s a real hierarchical organization usually.**
>
> **~ CSIRT member**

We want to add that differences in national cultures are not absolute and people within similar cultures can differ greatly in how they communicate within their teams. Also, there are many examples of smooth and successful communications across cultural boundaries in CSIRTs. However, several of our interviews with cybersecurity professionals revealed the cross-cultural communication issues described here. In those teams, managers acknowledged the need to address culture in communication protocols and its importance to conflict management.

In the next section, we review findings from our project related to CSIRT communication. This evidence, in combination with the above information, supports our later recommendations to enhance effective CSIRT communication.

5.2.2 PROJECT FINDINGS

According to our interviews and surveys with CSIRT members, the importance of communication processes and skills were confirmed for CSIRT work. All performance functions at the team and MTS levels of our developed taxonomy (see Appendix A) include communication activities. To summarize how focus group members and interviewees identified the importance of communication activities, and to provide examples of common communication practices most often endorsed, we framed examples according to a simplified incident response cycle (i.e., respond to incident, triage, develop solutions, and conduct after-action review). Table 5.2 presents the percentage of focus groups or interviews with cybersecurity professionals and managers that endorsed communication practices in each category. Within this framework, the most commonly identified communication practices and behaviors for team effectiveness were in the incident response and triage phases.

TABLE 5.2 INCIDENT RESPONSE CYCLE COMMUNICATION EXAMPLES

INCIDENT RESPONSE CYCLE PHASE	KEY COMMUNICATION THEMES IDENTIFIED BY FOCUS GROUP OR INTERVIEW PARTICIPANTS	PERCENTAGE OF FOCUS GROUP / INTERVIEWS (OUT OF 43)
Respond to incident	Discussion of how to share work; communication with affected constituency and stakeholders outside of constituency	88%
Triage	Discussion of how to assess and categorize identified incidents; information exchange to develop a shared understanding of the incident	65%
Develop solutions	Information exchange between teams to develop a shared understanding of incident; idea development between teams to select a course of action	60%
Conduct after-action review	Information exchange to evaluate procedures; revision of policies/procedures if necessary; determine necessary after-action adaptation strategies	42%

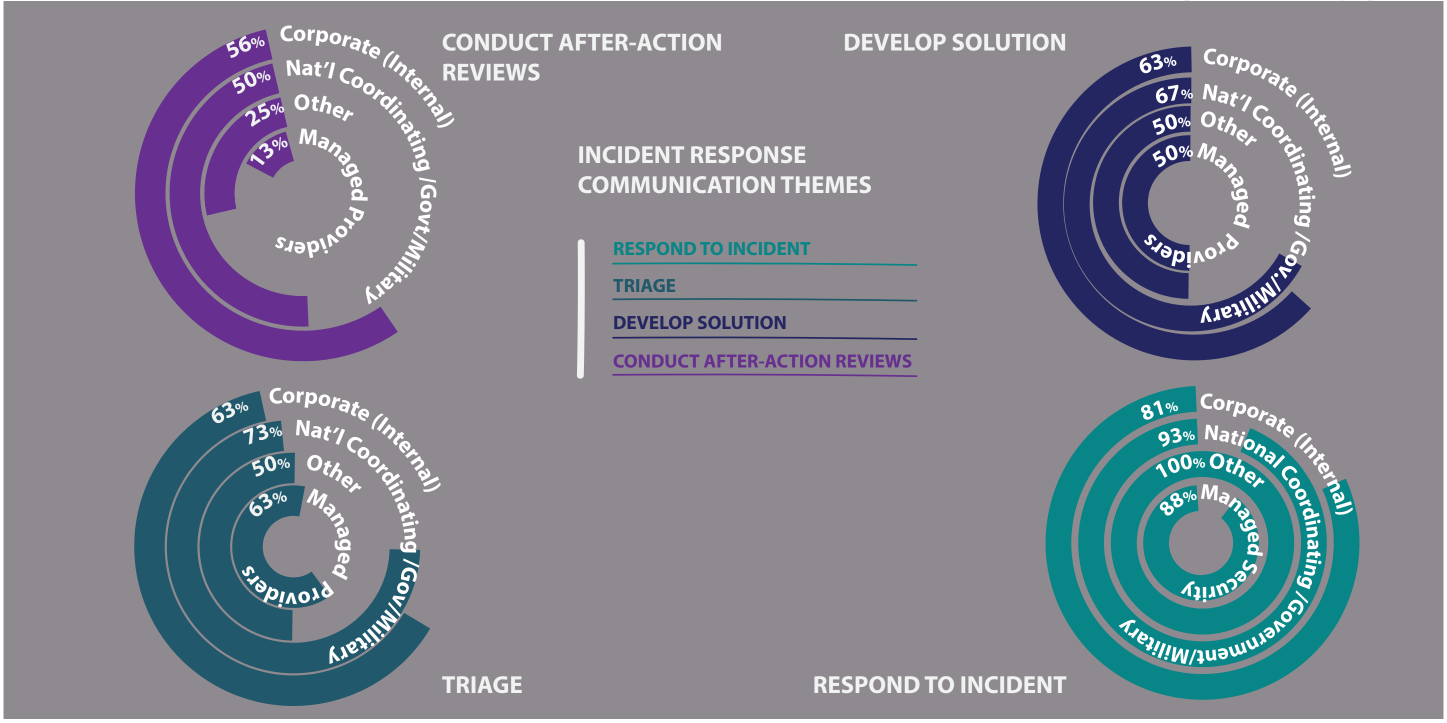


Figure 5.2 Endorsement of Communication Themes by CSIRT Type.

Note: Total Focus Groups (N=43); National Coordinating/Gov't/Military (N=15); Managed Security Service Providers(N=8); Corporate (N=16); Other (N=4).

TABLE 5.3 COMMUNICATION PRINCIPLES AND STRATEGIES TO IMPROVE THEM

PRINCIPLES	TRAINING STRATEGIES
Relevance	Handoff checklists, charters, tabular display, simulation
Quality	Handoff checklists, wikis, boundary spanning
Timeliness	Handoff checklists, charters, scenario-based training, simulation
Frequency	Charters, tabular display, scenario-based training, simulation, boundary spanning, workspace design
Information flow	Scenario-based training, simulation, tabular display, charters, boundary spanning, workspace design
Confirmation and response	Handoff checklists, scenario-based, simulation

We found other communication practices and behaviors within the "develop solutions" and "conduct after-action review" phases that were commonly identified as important for MTS effectiveness.

Figure 5.2 indicates the percentages of focus groups that mentioned the importance of communication processes in particular incident response phases. These percentages are indicated by type of CSIRT. All types of CSIRTs (i.e., coordinating, corporate, managed security service providers, and other) mentioned the use of one or more communication processes as important to the incident response process. They confirmed the criticality of communication throughout incident response.

The importance of communication skills for effective incident response was also reflected in our examination of 111 cybersecurity job ads and in a survey distributed to 88 cybersecurity professionals. Communication skills were one of the few social skills required of job candidates mentioned in the job ads. The survey asked cybersecurity professionals to rate 46 knowledge, skills, abilities, and other attributes (KSAOs) on their importance for performing well as a cybersecurity analyst. In that survey, 99% of respondents indicated that communication skills were important. Indeed, the ability to communicate effectively is the only social skill that appeared across previous job ads, our KSAO survey, *and* in focus group interviews, attesting to its prime importance to CSIRT performance.

5.3 Developing Communication Skills in CSIRTs

In this section, we provide strategies CSIRT managers can use to improve communication at multiple levels. CSIRT leaders and managers can implement all of these strategies, or they can choose particular strategies that make the most sense for their teams based on particular needs identified by them. Table 5.3 provides each communication principle and the strategies that enhance those principles. Managers and leaders should choose those strategies that target the communication principles where improvement is needed.

5.3.1 STRATEGY 1: REQUIRE TEAMS OR MTSs TO COMPLETE A TEAM CHARTER TO PLAN HOW, BETWEEN WHOM, AND WHEN COMMUNICATION WILL HAPPEN

Team charters define team expectations about how members are expected to interact with one another in defined situations (Mathieu & Rapp, 2009). These expectations emerge from team discussions. Team communication charters target the communication principles of frequency, timeliness, information flow, relevance of sent information, and confirmation the message was received. Managers can find examples and templates for team charters at: https://www.mindtools.com/pages/article/newTMM_95.htm. For more specific information on team communication charters, see: https://www.mindtools.com/pages/article/developing-communications-charter.htm.

Recommendations for use:

Team charters are created during team planning sessions to determine how the team will accomplish future work (Aaron, McDowell & Herdman, 2014). Such charters can be used to develop communication norms and expectations within the team (Mathieu & Rapp, 2009). The following is an example of communication processes team members should focus on in a team charter session:

Communication Plan Example

- What information do people need to know?
- How should this information be provided?
- Who will provide this information?
- When should information be provided?
- How will we share information with one another?
- How will we share information with other teams? Other organizations?
- What information can we share with other teams? Other organizations?
- Who will provide information to other teams? Other organizations?
- How do we need to adapt these processes under high time-pressure?
- What information is necessary in high-severity situations?

For dispersed teams, charters should also provide guidance on which communication method best matches the message content necessary to convey. For example, phone calls may be best if the message is urgent and personal, progress updates might be accomplished best through email (if immediate feedback is not needed), and group decisions can be more productive via video conferences (particularly if the parties are already well-known to one another). Team members also need to establish the frequency by which these different types of exchanges should happen between individuals or other teams. Charters should also set guidelines regarding communication protocols for when teams face high time demands or need to communicate with members from teams and MTSs that are physically or temporally dispersed (see Section 5.3.2 on handoff checklists).

Research has shown that communication charters help teams increase frequency and openness of communication (e.g., sharing relevant information with team members in a timely manner) by 18% and by as much as 25% when a leader or facilitator acts as an instructor and helps the team develop the charter (Aaron, et al., 2014). CSIRT managers who ensure that team members understand charter contents, and work to mitigate any conflict that arises during discussion, can increase the value of team charter use (Aaron, et al., 2014).

Charters also are useful for MTSs (Asencio, Carter, DeChurch, Zaccaro & Fiore, 2012). MTS charters specify communication norms *between teams* and establish protocols that multiple MTS component teams can use to communicate as they work together. The questions offered above (with greater emphasis on between team communications) can help guide the development of MTS charters.

Charter Considerations for Multicultural Teams

We noted earlier that one particular barrier to communication can be cultural differences. For example, one culture's conversational norms might be viewed as uncomfortable or offensive to members from another culture. Teams and MTSs need to explicitly be aware of such differences in conversational norms. Charters provide a framework for discussion and can ensure that cultural differences do not hinder team or MTS communication. In addition to regular communication plans discussed in team charters, the following communication norms might differ across cultures (e.g., different nations or organizations) and should be discussed explicitly in a face-to-face meeting of all team members and teams that will work together (Koehler, 2009):

- Length of emails
- Acceptable response (e.g., email response time)
- Frequency of communication
- Rules for greeting others
- Exchange of personal information
- Expression of personal feelings
- How to provide feedback
- How to express opinions and disagreement
- How members should refer to one another
- How members should build on one another's contributions
- Whether members should provide additional information and background when sending information
- How to ask questions (e.g., number of questions, type of questions, etc.)

The charter approach can be highly effective for multicultural teams. Multicultural teams that hold chartering meetings early during team development can be more successful at information sharing and communication, compared to teams that meet later, because early meetings contribute 30%-40% to team cooperation (Chatman & Flynn, 2001). Further, when multicultural teams increase face-to-face communication, conflict about how to complete tasks decreases significantly (Mortensen & Hinds, 2001).

5.3.2 STRATEGY 2: IMPLEMENT CHECKLISTS AND HANDOFF TOOLS TO PREVENT INFORMATION LOSS DURING HANDOFFS

Handoff tools are communication devices that provide structure to the handoff process so team members and/or teams can ensure they provide the most accurate and relevant information to others who take over responsibility for an incident or case. Examples of useful handoff tools include the SHARED and SBAR methods described below.

Recommendations for use:

Emergency response teams use the term "SHARED" at emergency scenes to make sure all relevant information is provided to all team members involved in the event (Riesenberg, Leitzsch, & Little, 2009). The acronym SHARED (**S**ituation, **H**istory, **A**ssessment, **R**isks, **E**vents, and **D**ocumentation) provides a tool for teams to share information quickly and effectively, as they must identify the information corresponding to each letter. SHARED is a type of pre-briefing (Section 5.4.2), which has been shown to significantly decrease mistakes in medical teams (Capella, Smith, & Philp et al., 2010; Gujsenbergh, Nieuwenhof, & Machiels, 2003).

Healthcare teams created the handoff tool "SBAR" (**S**ituation, **B**ackground, **A**ssessment, **R**ecommendation; Hamilton, Gemeinhardt, Mancuso, Sahlin, & Ivy, 2006). SBAR transmits, to other healthcare providers or teams, critical patient information, including status updates, key medical issues, and treatment recommendations (See Appendix E). SBAR structures information for the recipient while making sure that the person handing off the patient provides all relevant information the receiver needs in order to pick up where the other caregivers left off. With use of SBAR, the rate of adverse events in a hospital decreased by 40 per 1000 patient days (Haig, Sutton & Whittington, 2006). This process can easily be adapted to CSIRTs:

Situation: Current status of the incident (e.g., Has a network been penetrated?)

Background: Context information surrounding the incident (e.g., What do we know? How did this happen?)

Assessment: What is the severity of the problem?

Recommendation: Based on the problem and severity, what needs to happen next?

A communication guidance tool, such as SBAR, allows the handoff to be as smooth as possible without any time loss due to teams or team members seeking additional information or repeating already completed activities. Other considerations, beyond SBAR, that CSIRTs can include in handoff checklists are:

- Team members involved in the incident
- Work completed so far on incident resolution
- Details about location of supplemental materials
- Suggestions on how to proceed
- Timeline of mitigation actions taken so far
- Potential challenges that might arise with further incident mitigation

A third checklist possibility for CSIRTs can be borrowed from the change management field in the form of an iterative cycle called the Deming cycle (Deming, 2000), or a Plan, Do, Check, Act (PDCA) cycle. The PDCA cycle is designed as a model for continuous improvement and can be used to check the implementation of an incident response plan (Markey, 2012):

- **Plan**: The CSIRT must have a detailed plan for incident mitigation or resolution. The plan must include goals, work assignments, and an action plan based on the assignments.
- **Do**: The CSIRT members can now implement the plan. During this implementation phase, CSIRT members keep a list of issues or problems and use that list to improve the cycle.
- **Check**: The CSIRT uses the check phase to go through the list of issues that they encountered during incident response and discuss solutions.
- **Act**: Now the CSIRT is ready to implement the solutions that they developed in the check phase. Part of the acting phase is creating a standard set of procedures to ensure that the same problems do not resurface.

PDCA can be used to improve the entire incident response process, whereas checklists are targeted for a specific moment in the incident response cycle. Checklists can be incorporated at all phases of the PDCA cycle. CSIRT members and leaders indicated during our interviews that tools and checklists to prevent information loss are not often used to their full extent. Below, we offer a strategy to incorporate these tools and ensure they are used appropriately.

Implementation Recommendations:

Handoff checklists and the PDCA cycle can be implemented in several ways. They can be demonstrated to team and MTS members either using video presentation of effective versus ineffective use or by providing case study examples (Gillespie, Chaboyer, Longbottom & Wallis, 2010). If resources permit, use of handoff checklists should be practiced in scenario-based training exercises. CSIRT managers should describe the procedure and provide examples of how it can be used in daily communications. Checklists can then be integrated into reporting documents used by different teams and team members, including incident reports, handoff reports, strategic goal reporting, or simply used as a stand-a-lone tool.

After handoff checklists have been implemented, managers should periodically hold lessons-learned meetings and discuss ways to improve the use of the procedure within their teams or organizations; the PDCA cycle can be used to facilitate these conversations. After-action reviews enable CSIRTs to discuss particular instances where the procedure was used, what went well, and what should be improved (Haig et al., 2006). This type of discussion can increase buy-in and encourage continued use. Handoff checklists offer large benefits to improved communication relative to their resource costs.

5.3.3 STRATEGY 3A: USE SCENARIO-BASED TRAINING APPROACHES TO ENGAGE MEMBERS IN ROLE-PLAY

A more costly method than team charters is scenario-based training. All communication principles, as well as communication strategies and tools to improve communication, can be targeted with scenario-based training. This type of training uses communication scenarios to help team members practice communication protocols and the use of particular communication tools. Such training can also be used to help different teams in a CSIRT MTS learn and practice between-team communication protocols and tools. After training, CSIRT managers should provide feedback to guide members in the continued use of relevant communication skills as well as point out strengths and areas for improvement.

Other considerations for scenario-based training include follow-up meetings where team and MTS members discuss situations in which they used trained skills. These discussions can increase knowledge retention and motivate continued practice of learned skills. One training program in particular, the TeamSTEPPS program, was initially created to improve teamwork and patient safety among healthcare teams (Robertson, et al., 2010). This program offers the following communication tools and strategies that can be modified to the cybersecurity domain (please see teamstepps.ahrq.gov for descriptions of these tools along with training materials to develop skills in using them):

- Pre-brief (initial planning meeting; see Chapter 7, “Collaborative Problem Solving in Incident Response”)
- Huddle (meetings during action phases to check and adjust plans)
- Handoff tools (SBAR and SHARED; described in detail in section 5.2.3)
- Call-outs (used to provide relevant and timely information)
- Check-backs (used to provide receiver confirmation and response)
- SMARTT step-back procedure (Roberts et al., 2014, p. 173): Step back from the situation to prevent members from fixating on one aspect or idea
    - "**S**ituation (case or incident description, severity, status, circumstances)"
    - "**M**anagement (action taken)"
    - "Activity (what needs to happen next?)"
    - "**R**apidity (what needs to be done first and how quickly?)"
    - "**T**roubleshoot (what can go wrong and steps to correct or prevent)"
    - "**T**alk to me (encourage all team members to volunteer key information, ask clarifying questions) "

Recommendations for use:

Below, we provide one scenario-based training protocol example, based on the TeamSTEPPS program (Harvey, Echols, Clark & Lee, 2014; Hughes et al., 2014; Roberts et al., 2014), to develop communication skills and use communication tools:

Step 1: Participants observe a communication interaction (typically a video clip) relevant to the specific principle or tool and strategies targeted, including instructions about behaviors that reflect that principle. This type of presentation should also include examples of effective and ineffective uses of specific tools or skills (Hughes et al., 2014). Separate clips should be used for within and between team communications.

Step 2 (Optional): Participants can discuss the communication skills they observed and set their own goals for developing those skills. Team members should identify specific CSIRT-related instances where they expect to use and practice developing the skill. Leaders can provide specific feedback about communication skills in this step.

Step 3: Team members practice skills by engaging in role-play in small groups, using the tactics described in the video. Specifically, all team members are assigned roles and tasks where they must use the desired communication skills or tools. Role-play should reflect realistic scenarios that members might encounter in their work. For CSIRTs, scenarios could include reenacting a past incident or creating entirely new incidents. Leaders or facilitators should observe this process.

Step 4: The leader or facilitator who observes the role play provides feedback to team members on their use of particular skills and helps develop an action plan for how each team member can apply that skill at work.

Step 5: Managers should check with participants in several weeks post-training to discuss participants' progress and any opportunities they had to practice and develop their skills.

This form of scenario-based training is effective in many different contexts. Individuals in medical teams reported 50-60% improvement in communication skills related to engaging in difficult conversations with patients; that improvement lasted at least 5 months after training (Meyer et al., 2009). Medical teams trained to use communication pre-brief, huddle, call-outs and handoff tools (e.g., TeamSTEPPS) increased communication skills, such as sharing information as soon as it was available, by 16% (Robertson et al., 2010). Other medical teams using this approach saw a 23-129% increase in skills such as acknowledging messages, clarifying messages, and displaying checking-back behaviors with teammates to whom they conveyed information (Langewitz, Eich, Kiss & Wossimer, 1998).

Combine Pre-briefing with Scenario-based Training

Pre-briefing (see Chapter 7, "Collaborative Problem Solving in Incident Response") can be used in conjunction with scenario-based training to build communication skills. To incorporate this procedure in scenario-based training, managers conduct a pre-briefing before team members begin to engage in role-play. This process is essentially a brief planning session to get all members on the same page before they begin interacting to solve the problem scenario. This process is similar to the SMARTT step-back procedure, where members identify relevant persons, tasks, and resources so that all members understand important information related to the incident and raise any questions or concerns for group discussion.

Research has shown that pre-briefings before engagement in role-play contributed to improved communication quality during patient care by 10% in a medical team scenario-based training (Hughes et al., 2014). Importantly, conveying relevant information in a timely manner before beginning care increased by 33% and providing updates throughout care increased from 8% before training to 71% after training. Verbalization of response plans during pre-briefing increased from 44% before training to 89% after teams were trained in the method (Hughes et al. 2014). These data indicate that combined pre-briefing and scenario-based training can yield extreme benefits relative to their typically low costs. Pre-briefings also can be used to determine the handoff tools team members should use, as described in the next section. Handoff tools can be implemented in scenario-based team trainings for practice (See Appendix D for an example of a Program of Instruction to train communication skills).

5.3.4 STRATEGY 3B: ENGAGE TEAMS AND MTSs IN SIMULATION-BASED TRAINING

Team/MTS Simulation training

Similar to scenario-based training, simulation training engages members of teams and/or MTSs in solving a simulated incident, but the simulation is more intense and involved than scenario role-play. Stages of simulation-based training can include:

- Presentation of the targeted communication principles
- Practice of targeted communication principles across a variety of different, and increasingly challenging, incident response scenarios
- Provision of feedback during and after practice scenarios
- Team discussions of lessons learned in each practice scenario
- Team discussions of how to extend lessons learned to the workplace, including potential obstacles, in order to ensure that the training is used on the job

A popular example of simulation training is crew resource management (Salas, Rhodenizer, & Bowers, 2000). Crew resource management was first implemented in aviation teams, but the core goal of the training is communication improvement. Crew resource management and other similar simulation-based training programs engage team members in realistic crisis scenarios where they must coordinate their actions to resolve the crisis (Hughes et al., 2014). In such simulations, team members can use different types of communication channels (e.g., radios, telephones, group chat, and video-conferencing) during the simulation exercise. If all team members are located in the same physical space, simulations might not require the full range of such technology, but they should resemble crisis situations or major incidents where team members must provide different types of communications at different phases of the incident response process. Simulations should contain learning objectives and instructor/facilitator guidance and feedback (Douglass, Casale, Skirvin, & DiVall, 2013), and should demonstrate maximal realism and fidelity to actual incident response situations, including the typical technologies used in these situations. Simulations also can include pre-briefings, as well as debriefings, which focus specifically on team communication. Debriefings provide feedback to teams regarding what went well, what went wrong, and how communication principles can be applied to everyday work (Douglass et al., 2013).

Simulations effectively improve communication skills. In a simulation training for medical teams (Roberts et al., 2014), the SMARTT step-back procedure immediately improved the following communication skills (percent improvement): volunteering important information (49%); active listening (25%); confirmation of completed tasks (62%); asking for clarification (59%); leader coordination of team communication and team activity (48%); leader management of distracting communication (45%); and leader encouragement of team members to volunteer key information during the SMARTT step-back procedure (139%). The improvement demonstrated after training remained evident three weeks post-training (Roberts et al., 2014).

Simulation programs have demonstrated significant improvements in overall communication (16%); orienting new team members using SBAR (described earlier; 17%); transparent thinking (16%); directed communication (assert oneself respectfully to ensure information is heard; 19%); and closed-loop communication (use of structured communication tools; 18%; Paull et al., 2013). Overall communication increased in a similar simulation-based training using the TeamSTEPPS curricula (Harvey et al., 2014).

5.3.5 STRATEGY 4A: DESIGN A VIRTUAL DISPLAY THAT ALL TEAM MEMBERS CAN USE TO MONITOR INFORMATION

When CSIRTs are distributed or virtual, they communicate via several tools. One such tool, a virtual display board in which team members can post and view information, is a passive method of communication (Strang, Funke, Knott, Galster, & Russell, 2011). All members of the team or MTS can access and continually monitor virtual display boards.

Recommendations for Use:

The information displayed can inform team members of work completed on an incident. When all team members can view and monitor this information, they share situational awareness. A unique aspect of this strategy is that it reduces the need for teams to communicate actively about this information because the information is continually available to everyone (Strang et al., 2011).

A training study tested the use of such information boards in military teams. In a battle training simulation, teams were required to coordinate their activities to fight off enemy attacks. A display board was implemented where all members could post and monitor resource information. Teams spent, on average, 19% less time communicating by radio when they had a display board, with no decrement in performance (Strang, et al., 2011).

5.3.6 STRATEGY 4B: APPLY BEST PRACTICES TO MAKE WIKIS MORE EFFECTIVE

Recommendations for use:

Much like display boards or virtual whiteboards, wikis are well-suited for tracking information and maintaining situational awareness. Wikis can be effective tools for communication.

Recommendations for use:

Display boards are generally best used to communicate and monitor incident-specific information during a particular incident, whereas wikis are repositories for all relevant information the team might need to track. Wikis allow for collaboration among multiple authors through the sending and receiving of information in a virtual environment, allow individuals to send information on a broader scale (e.g., to more than one person), as well as document pieces of information related to threats, attacks, hackers, incident response processes or other important material that can be referenced later. Wikis can be particularly useful to track trends and threats because patterns are easier to notice when information is viewed across several days, weeks, or months.

Wikis and virtual whiteboards are only helpful to CSIRTs if they are maintained and used by all members of the team. Likewise, all teams in a CSIRT MTS would need to contribute and support established wikis. Some best practices that have helped increase the impact of wikis include (Wagner, 2004):

- The wiki is used for ad-hoc problems that require knowledge from different sources;
- The wiki uses a mark-up scheme with which all team members are familiar (e.g., a simplified version of HTML);
- Wiki content can be updated by any team member and can accommodate incremental contributions;
- The wiki is not reviewed by the manager or any other

> **“They are the one that straddles across everything because they're there to make sure that the communication, not only between the teams but out to our partners whether they're industry, government or international [partners], so they help across every single one of those strands.”**
>
> **~ CSIRT member**

senior staff member prior to publication on the wiki; and

- The wiki employs an effective search tool to enable users to find content quickly.

Wagner (2004) offered several other suggestions to increase the utility and effectiveness of a wiki tool. He argued that wikis should be constructed in ways that allow readers and users to edit the material at will and to cite other pages in the wiki. The wiki should facilitate constant evolution of material. There should minimal duplication of information in the wiki, and the wiki should be easily accessible by all users. These, and other principles, are described in more detail by Wagner (2004), a copy of which can be acquired at http://aisel.aisnet.org/cais/vol13/iss1/19/.

CONSIDERATIONS FOR COMMUNICATION BETWEEN TEAMS AND EXTERNAL PARTIES

5.3.7 STRATEGY 5: ASSIGN A TEAM MEMBER TO ACT AS THE POINT OF CONTACT FOR BETWEEN-TEAM COMMUNICATION IN A CSIRT MTS

The principles for effective communication *within* teams do not necessarily apply equally to communications *between* teams in an MTS. When CSIRTs need to coordinate between team actions in a crisis situation, having too many people from different component teams communicate with one another can be chaotic and subsequently hurt the overall performance of the MTS (Davison, Hollenbeck, Barnes, Sleesman & Ilgen, 2012). One strategy to minimize such chaos and confusion is to assign a specific person to handle communication with other component teams (a "boundary spanner").

Boundary spanning refers to a team's efforts to establish and maintain linkages with other individuals or teams outside their own team, both internal and external to the organization (Ancona, 1990). Boundary spanning has a wide array of functions, including seeking information from and communicating information to external parties, setting objectives and managing expectations, providing status updates, connecting with individuals or teams who can provide desired resources, and any other type of interaction outside team boundaries (Marrone, 2010). In CSIRTs, boundary spanning activities can include making queries for additional information from another team within the MTS, responding to recommendations, and providing information to help coordinate and report incident response progress to external stakeholders (Alberts, Dorofee, Killcrece, Ruefle & Zajicek, 2004). The impact that boundary spanning can have on MTS communication is discussed here, but a full explanation of MTS considerations can be found in Chapter 2, "The Social Maturity of CSIRTs and Multiteam Systems."

While boundary spanning is critical to the performance of teams and MTSs, it can be difficult and taxing work. Leaders and managers can take certain steps to ensure that the right team member takes on the boundary spanning role and succeeds. Team boundary spanners should be selected based on their motivation, experience, and confidence in their ability to take on this role (Ancona & Caldwell, 1990). Support from leadership, in the form of coaching behaviors, helps ensure that boundary spanning happens effectively (Edmondson, 2003). Below, we outline a specific approach to ensure that boundary spanning has the intended benefits (Edmondson, Roberto & Watkins, 2003; Marrone et al., 2007).

Recommendations for use:

- Select a highly motivated team member to take ownership of communication with other teams in the MTS and outside stakeholders (i.e., act as the team boundary spanner).
- Clearly define the scope of the boundary spanner role and enable the boundary spanning team member to take ownership of the task. The team member must be comfortable with the responsibilities of a boundary spanner (e.g., relaying information, seeking information, providing progress updates to outside stakeholders).
- Review boundary spanning ideas and suggestions from the designated team member and provide specific, actionable feedback.
- Communicate the team member's boundary spanning role to the entire team so that team members know who is responsible for what activities and can direct questions and requests for other teams to the right person.
- Provide feedback specific to boundary spanning individuals after witnessing their performance during an incident so he or she can identify areas for improvement, as well as what was done well.

CONSIDERATIONS FOR THE PHYSICAL WORK SPACE

5.3.8 STRATEGY 6: DESIGN THE WORK SPACE TO INCREASE COMMUNICATION

The layout of the physical workspace can significantly influence team communication (Kupritz & Hillsman, 2011). When the workspace is open, and team members are located near one another without physical barriers (e.g., walls), communication occurs more easily and more frequently (De Paoli, Arge, & Hunnes Blaksted, 2013; Robertson, Huang, O'Neil, & Schleifer, 2008). One thing to consider is that while open workspaces have benefits for certain types of jobs, such as those that involve knowledge work, not every person works best in this type of environment. Managers can incorporate private zones into their work designs, or give employees some freedom to choose where they want to work. Specific rooms can be designated for group discussion, preventing noise distractions during working hours (De Paoli, et al., 2013).

Recommendations for Use:

In our focus groups and interviews, we asked managers of

> **We know each other; we're in the same room; we know who does what. So it's very easy to communicate about incidents and things like that.**
>
> **~ CSIRT member**

effective CSIRTs to tell us how they designed their workspace. In one case, a manager designed a space in which the entire team was in the same room to facilitate open lines of communication. Other cybersecurity professionals we interviewed utilized a specific room by populating it with members of different component teams so that they could easily communicate important information across teams, as well as synchronize their actions. These teams needed to closely interact in order to provide constituents with threat information; therefore, being physically close greatly increased their ability to do so. Physical proximity is important for both informal conversations and information sharing in CSIRTs (Alberts et al., 2004).

In our research, we observed a CSIRT manager who had the opportunity to design a space built around communication. In this workspace, analysts sat in a shared, open office environment but had the option to move to a more private "cyber consultation center" for meetings and deeper discussion of particular incidents. Additionally, this particular office was equipped with video conferencing capability to facilitate collaboration between teams in the CSIRT that were not physically located in the same place.

Based on our research, and findings from other studies of workplace design and communication effectiveness (e.g., De Paoli, et al., 2013; De Paoli & Ropo, 2015; Robertson, et al., 2008), we suggest that CSIRT workspaces include the following features:

- An operations area where analysts work at open desks, or partitioned carrels, arranged to facilitate both open communication and individual work
- A flexible space where furniture can be rearranged or reconfigured to fit different CSIRT needs
- Work surfaces large enough to spread out multiple work documents
- Separate, open, informal meeting spaces for quick consultations
- Separate, enclosed, formal meeting spaces of varying sizes that can accommodate more private meetings involving (a) two people, (b) multiple team members, or (c) multiple small teams
- Video conferencing capabilities for communication with other analysts and teams in other physical locations

Effectiveness Evidence:

Evidence suggests that open workspace designs positively influence communication when employees are offered recommendations and guidelines for how to utilize the space. Employees introduced to a flexible and open workspace had 10% more face-to-face interactions with coworkers and 10% higher ease of collaboration than those without such workspaces (Robertson et al., 2008). They also had significantly higher instances of communication and collaboration after using the work stations than they did before they were introduced to them (Robertson et al., 2008).

Workspace layout has implications not only for communication frequency as well as openness and information flow, but also for the effectiveness of scenario and simulation-based communication training. A case study of a large company revealed that one of the most important factors for supervisors utilizing their skills after they completed a communication training exercise was the design of the workplace (Kupritz & Hillsman, 2011). In this exercise, supervisors were taught effective listening and feedback-giving. Features of the workspace that positively influenced their ability to use these skills included having a quiet place to give feedback, having a convenient group meeting space, close proximity to team members, and an open design. Managers felt that poor proximity to team members inhibited their ability to work as a team (Kupritz & Hillsman, 2011).

> **We have the advanced threats [analysts] that literally sit 3 feet from us. I'll turn around and talk to them or walk over to them and say, 'Hey, can you come look at my screen?' It's easier to do that a lot of times than take screen shots and send it over to whomever.**
>
> **~ CSIRT member**

5.3.9 STRATEGY 7: MAKE TEAM STAFFING DECISIONS BY USING SITUATIONAL INTERVIEWS TO ASSESS COMMUNICATION SKILLS

Situational interviewing is a technique used to encourage job applicants to describe how they have handled specific work situations in the past. The interviewer asks job candidates a predetermined, standard set of questions focused on past behaviors and experiences that will enable interviewees to showcase the knowledge, skills, or abilities they will need to be successful on the job (Pulakos & Schmitt, 1995). The key to situational interviewing is the underlying notion that past performance in similar situations predicts future performance (Latham, Saari, Pursell, & Campion, 1980). Asking job candidates how they have solved problems and handled past challenges that they are likely to also encounter on the job can determine if the candidate has the experience to be successful.

Recommendations for use:

- Use situational interviewing techniques when selecting potential new CSIRT members, ensuring that all interviewees receive the same question so that responses can be directly compared.
- Determine the communication-related situations that are most critical to CSIRT success and that the new team member is most likely to encounter on the job.
- To create situational interview questions that measure

communication skills, review the principles in this chapter and write questions that address the specific principle(s) that you believe your team needs. The questions you write should give applicants the opportunity to describe how they handled a specific situation and to describe the outcome of their actions.

- When scoring responses to situational interview questions, have two interviewers in the room. Both should rate the response on a 1-5 scale (1 being poor; 5 being excellent) and then discuss their reasons for assigning a particular score during the interview. It may be helpful to take notes during the interview so it is easier to remember the exact reasons for assigning a particular score.

Situational Interview Sample Questions and Responses

We have designed the following three sample questions as suggestions for assessing an applicant's skill in demonstrating the communication principles of quality (principle #1), timeliness (principle #3), and information flow (principle #5). They can be adapted to cover the other communication principles or topics beyond communication but are meant to serve as a starting point to help CSIRT managers write their own situational interview questions. Please note that the situation interview questions below have not undergone the necessary rigorous validation process (see Appendix C, "Hiring and Training CSIRT Employees: Validation Consideration”). They are only intended to provide CSIRT managers with an idea for the types of situational interview questions that can be used to measure applicant communication skills. Managers should refer to their Human Resource Management departments for additional information about validation of such items.

Question 1: Describe a situation in which you had to prepare an incident briefing for others in your CSIRT. How did you ensure that you provided accurate information that would be helpful for them to continue working on the incident? Be as specific as possible when describing your actions and their outcomes. If you have not had experience preparing an incident briefing, please describe an experience in which you had to ensure accurate information was conveyed to a team member.

QUESTION 1

ELEMENTS OF STRONG RESPONSES	RED FLAG RESPONSES
Response contains all of the details (includes description of situation, the background, an assessment of what is needed, and recommendations on next steps for resolution)	Response where one might infer a lack of information organization - fails to mention specific incident details (e.g., background, needs assessment, or recommended next steps, if applicable)
Points out novel and/or critical elements of situation	Mentions using standard template without providing information about details
Mentions double-checking or checking with others for accuracy	Does not mention checking with others or double-checking for accuracy
Mentions positive response from others who received the report	Mentions others who received report providing negative responses or coming back for clarification
Mentions how briefing or other reporting helped others to mitigate incident or other positive outcomes	Mentions providing/preparing report was a waste of time

Question 2: Describe a situation in which you were handling an incident and you realized that it was time to involve another team in your CSIRT. How did you provide them with the most up-to-date information about the incident and how did this affect the incident resolution? Be as specific as possible when describing your actions and their outcomes. If you have not had this experience, please describe another time you had to involve others outside of your immediate work team when solving a problem.

QUESTION 2

ELEMENTS OF STRONG RESPONSES	RED FLAG RESPONSES
Mentions recognition of need for others to know information	Mentions delay in contacting a member from another group
Mentions how they knew who to contact or how they found out	Blames others, or organizational structure, for not knowing who to contact
Mentions timeliness of contact or the importance of timeliness in providing information to others outside the team	Mentions difficulty with collaboration due to contacting another team too early or too late
Mentions they provided information in an efficient matter (e.g., briefing with the appropriate stakeholders, if relevant)	Mentions they provided the information in an inefficient manner (e.g., sent an email without any followup)
Mentions positive interaction with other teams both during the interaction and as an outcome of the interaction	Mentions contacting others from another group was a waste of time or provides other negative attitudes about interaction
Speaks positively about interacting with other teams in the future	Mentions hesitancy to contact this group in the future

Question 3: Describe a situation in which you had to make a decision about which members of your CSIRT needed to be informed of an incident in progress. How did you determine the right team members to reach out to in the situation and what was the result? Be as specific as possible when describing your actions and their outcomes.

While situational interview questions do not have wrong answers, the elements of strong responses and the red flag responses above should help with scoring applicant responses to questions and differentiate between the strong and weak communication skills of various job applicants.

QUESTION 3	
ELEMENTS OF STRONG RESPONSES	**RED FLAG RESPONSES**
Mentions knowledge or importance of knowing all pertinent stakeholders who were relevant to situation described	Response where one might infer there was a lack of understanding who were the important stakeholders in this particular situation
Response indicates initiative taken to make sure right team members were contacted	Blames others, or organizational structure, for not knowing who to contact
Mentions contacting only pertinent stakeholders versus broader communication (e.g., mass email)	Mentions reaching out to others who did not need information
Mentions a positive interaction and/or outcome with those contacted in this situation	Mentions a negative interaction and/or outcome with those contacted in this situation
Mentions looking forward to future collaboration with those contacted	Mentions hesitancy to collaborate with those contacted in the future

5.4 Chapter Summary

Our survey indicates that effective communication is a top social skill for CSIRTs. The ability to send and receive messages according to the communication principles outlined in this chapter has important implications for the incident response process, and managers can use the strategies we provide to improve communication within their CSIRTs. Managers also need to consider the extent to which time demands, team dispersion, and cultural boundaries impact communication processes.

Effective communication also serves as a foundation for information sharing across individuals, teams, and MTSs. CSIRT managers can facilitate successful information sharing when they establish high quality communication protocols and train team members to use such protocols. In the next chapter, we expand upon the development of effective communication protocols for enhanced information sharing.

References

Aaron, J. R., McDowell, W. C., & Herdman, A. O. (2014). The effects of a team charter on student team behaviors. *Journal of Education for Business*, *89*(2), 90-97.

Aebersold, M., Tschannen, D., Sculli, G. (2013). Improving nursing students' communication skills using crew resource management strategies. *Journal of Nursing Education*, *52*(3), 125-130.

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). *Defining incident management processes for CSIRTs: A work in progress* (No. CMU/SEI-2004-TR-015). Carnegie-Mellon University, Pittsburgh, PA. Software Engineering Institute.

Ancona, D. G. (1990). Outward bound: Strategies for team survival in an organization. *Academy of Management Journal*, *33*, 334–365.

Ancona, D. G., & Caldwell, D. (1990). Beyond boundary spanning: Managing external dependence in product development teams. *The Journal of High Technology Management Research*, *1*(2), 119-135.

Asencio, R., Carter, D. R., DeChurch, L. A., Zaccaro, S. J., & Fiore, S. M. (2012). Charting a course for collaboration: A multiteam perspective. *Translational Behavioral Medicine*, *2*(4), 487-494.

Barrett, D., & Yadron, D. (2015, February 22). *Sony, U.S. Agencies Fumbled After Cyberattack*. Retrieved from http://www.wsj.com/articles/sony-u-s-agencies-fumbled-after-cyberattack-1424641424.

Berry, M., Carbaugh, D., Innreiter-Moser, C., Nurmikari-Berry, M., & Oetsch, W. (2009). *That's not me: Learning to cope with sensitive cultural issues*. Turku, Finland: Michael Berry.

Capella, J., Smith, S., Philp, A., Putnam, T., Gilbert, C., Fry, W. & ReMine, S. (2010). Teamwork training improves the clinical care of trauma patients. *Journal of surgical education*, *67*(6), 439-443.

Chatman, J. A., & Flynn, F. J. (2001). The influence of demographic heterogeneity on the emergence and consequences of cooperative norms in work teams. *Academy of Management Journal*, *44*(5), 956-974.

Davison, R. B., Hollenbeck, J. R., Barnes, C. M., Sleesman, D. J., & Ilgen, D. R. (2012). Coordinated action in multiteam systems. *Journal of Applied Psychology*, *97*(4), 808-824.

de Guinea, A. O., Webster, J., & Staples, D. S. (2012). A meta-analysis of the consequences of virtualness on team functioning. *Information & Management*,*49*(6), 301-308.

Deming, W. E. (2000). *Out of the crisis*. Cambridge, Mass.: MIT Press. 88.

De Paoli, D., Arge, K., & Hunnes Blakstad, S. (2013). Creating business value with open space flexible offices. *Journal of Corporate Real Estate, 15*(3/4), 181-193.

De Paoli, D.D., & Ropo, A. (2015). Open plan offices – the response to leadership challenges of virtual project work? *Journal of Corporate Real Estate*, *17*, 63-74.

Douglass M.A., Casale J.P., Skirvin A., & DiVall M.V. (2013). A virtual patient software program to improve pharmacy student learning in a comprehensive disease management course. *American Journal of Pharmaceutical Education, 77*, 172.

Edmondson, A. C. (2003). Speaking up in the operating room: How team leaders promote learning in interdisciplinary action teams. *Journal of Management Studies*, *40*(6), 1419-1452.

Edmondson, A. C., Roberto, M. A., & Watkins, M. D. (2003). A dynamic model of top management team effectiveness: Managing unstructured task streams. *The Leadership Quarterly*, *14*(3), 297-325.

Ford, D. P., & Chan, Y. E. (2003). Knowledge sharing in a multi-cultural setting: a case study. *Knowledge Management Research & Practice*, *1*(1), 11-27.

Gibson, C., & Vermeulen, F. (2003). A healthy divide: Subgroups as a stimulus for team learning behavior. *Administrative Science Quarterly*, *48*(2), 202-239.

Gijsenbergh, F., Nieuwenhof, A., & Machiels, K. (2003). Improving the first link in the chain of survival: the Antwerp experience. *European Journal of Emergency Medicine*, *10*(3), 189-194.

Gillespie, B. M., Chaboyer, W., Longbottom, P., & Wallis, M. (2010). The impact of organisational and individual factors on team communication in surgery: a qualitative study. *International Journal of Nursing Studies*, *47*(6), 732-741

Gladstein, D. L., & Reilly, N. P. (1985). Group decision making under threat: The tycoon game. *Academy of Management Journal*, *28*(3), 613-627.

Haig, K. M., Sutton, S., & Whittington, J. (2006). SBAR: a shared mental model for improving communication between clinicians. *Joint Commission Journal on Quality and Patient Safety*, *32*(3), 167-175.

Hall, J. A. (1979). Gender, gender roles, and nonverbal communication skills. In R. Rosenthal (Ed.), *Skill in nonverbal communication* (pp. 32-67). Cambridge, MA: Oelgeschlager, Gunn, & Hain.

Hambrick, D. C., Davison, S. C., Snell, S. A., & Snow, C. C. (1998). When groups consist of multiple nationalities: Towards a new understanding of the implications. *Organization Studies*, *19*(2), 181-205.

Hamilton, P., Gemeinhardt, G., Mancuso, P., Sahlin, C. L., & Ivy, L. (2006). SBAR and nurse-physician communication: Pilot testing an educational intervention. *Nursing Administration Quarterly*, *30*(3), 295-299.

Harvey, E. M., Echols, S. R., Clark, R., & Lee, E. (2014). Comparison of Two TeamSTEPPS® Training Methods on Nurse Failure-to-Rescue Performance. *Clinical Simulation in Nursing*, *10*(2), e57-e64.

Hofstede, G. (1984). *Culture's consequences: International differences in work-related values* (Vol. 5). Newbery Park, CA: Sage Publications.

Hofstede, G., Hofstede, G. J., & Minkov, J. (2010). *Cultures and organizations: Software of the mind (Revised and Expanded 3rd Edition)*. New York: McGraw-Hill USA.

Hughes, K. M., Benenson, R. S., Krichten, A. E., Clancy, K. D., Ryan, J. P., & Hammond, C. (2014). A crew resource management program tailored to trauma resuscitation improves team behavior and communication. *Journal of the*

American College of Surgeons, *219*(3), 545-551.

Hwang, Y., & Kim, D. J. (2007). Understanding affective commitment, collectivist culture, and social influence in relation to knowledge sharing in technology mediated learning. IEEE *Transactions on Professional Communication*, *50*(3), 232-248.

Koehler, T. (2009). *What role do norms play in global teamwork? The influence of cultural communication and coordination norms on team processes in internationally distributed teams* (Unpublished doctoral dissertation). George Mason University, Fairfax, VA.

Kupritz, V. W., & Hillsman, T. (2011). The impact of the physical environment on supervisory communication skills transfer. *Journal of Business Communication*, *48*(2), 148-185.

Lam, S. S., & Schaubroeck, J. (2000). Improving group decisions by better pooling information: A comparative advantage of group decision support systems. *Journal of Applied Psychology*, *85*(4), 565-573.

Langewitz, W. A., Eich, P., Kiss, A., & Wossmer, B. (1998). Improving communication skills-a randomized controlled behaviorally oriented intervention study for residents in internal medicine. *Psychosomatic Medicine, 60*(3), 268-276.

Latham, G.P., Saari, L.M., Pursell, E.D., & Campion, M.A. (1980). The situational interview. *Journal of Applied Psychology, 65*, 422-427

Markey, S. (2012). Testing your computer security incident response plan. *ISACA Journal*, *2*, 1-5.

Marrone, J. A. (2010). Team boundary spanning: A multilevel review of past research and proposals for the future. *Journal of Management*, 36(4), 911-940.

Marrone, J. A., Tesluk, P. E., & Carson, J. B. (2007). A multilevel investigation of antecedents and consequences of team member boundary-spanning behavior. *Academy of Management Journal*, *50*(6), 1423-1439.

Mathieu, J. E., & Rapp, T. L. (2009). Laying the foundation for successful team performance trajectories: The roles of team charters and performance strategies. *Journal of Applied Psychology*, *94*(1), 90-103.

Meyer, E. C., Sellers, D. E., Browning, D. M., McGuffie, K., Solomon, M. Z., & Truog, R. D. (2009). Difficult conversations: Improving communication skills and relational abilities in health care. *Pediatric Critical Care Medicine*, *10*(3), 352-359.

Ministry of Security and Justice of the Netherlands, Federal Office for Information Security of Germany, & Swedish Civil Contingencies Agency of Sweden (2014). *International case report on cyber security incidents: Reflections on three cyber incidents in the Netherlands, Germany and Sweden*. Retrieved from https://www.gccs2015.com/sites/default/files/documents/ICR_CYBERCECURITYINCIDENTS_LR.PDF

Mortensen, M., & Hinds, P. J. (2001). Conflict and shared identity in geographically distributed teams. *International Journal of Conflict Management*, *12*(3), 212-238.

Mortensen, M. & Hinds, P. (2001). Conflict and shared identity in geographically distributed teams. *International Journal of Conflict Management, 12(3)*, 212-238.

Nickerson, Raymond S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology 2*, 175–220.

Paull, D. E., DeLeeuw, L. D., Wolk, S., Paige, J. T., & Neily, J. (2013). The effect of simulation-based crew resource management training on measurable teamwork and communication among interprofessional teams caring for postoperative patients. *The Journal of Continuing Education in Nursing*, *44*(11), 516-524.

Pulakos, E.D., & Schmitt, N. (1995). Experience-based and situational interview questions: Studies of validity. *Personnel Psychology, 48*, 289-308

Rench, T., Horn, Z., Walker, A., & Zaccaro, S. (2014). Accelerating Unit Adaptability: A principle-based approach to unit communication. Presented at the Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC). Orlando, FL.

Riggio, R. E. (1986). Assessment of basic social skills. *Journal of Personality and Social Psychology*, *51*(3), 649-660.

Risenberg, L. A., Leitzsch, J., & Little, B. W. (2009). Systematic review of handoff mnemonics literature. *American Journal of Medical Quality, 24*, 196-204

Roberts, N. K., Williams, R. G., Schwind, C. J., Sutyak, J. A., McDowell, C., Griffen, D., ... & Wetter, N. (2014). The impact of brief team communication, leadership and team behavior training on ad hoc team performance in trauma care settings. *The American Journal of Surgery, 207*(2), 170-178.

Robertson, M. M., Huang, Y. H., O'Neill, M. J., & Schleifer, L. M. (2008). Flexible workspace design and ergonomics training: Impacts on the psychosocial work environment, musculoskeletal health, and work effectiveness among knowledge workers. *Applied Ergonomics, 39*(4), 482-494.

Robertson, B., Kaplan, B., Atallah, H., Higgins, M., Lewitt, M. J., & Ander, D. S. (2010). The use of simulation and a modified TeamSTEPPS curriculum for medical and nursing student team training. *Simulation in Healthcare*, *5*(6), 332-337.

Salas, E., Rhodenizer, L., & Bowers, C. A. (2000). The design and delivery of crew resource management training: exploiting available resources. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 42*(3), 490-511.

Stasser, G., Taylor, L. A., & Hanna, C. (1989). Information sampling in structured and unstructured discussions of three-and six-person groups. *Journal of Personality and Social Psychology*, *57*(1), 67-78.

Strang, A. J., Funke, G. J., Knott, B. A., Galster, S. M., & Russell, S. M. (2012, September). Effects of cross-training on team performance, communication, and workload in simulated air battle management. In *Proceedings of the Human Factors and Ergonomics Society 56th Annual Meeting* (pp. 1581-1585). Dayton, OH: HFSE.

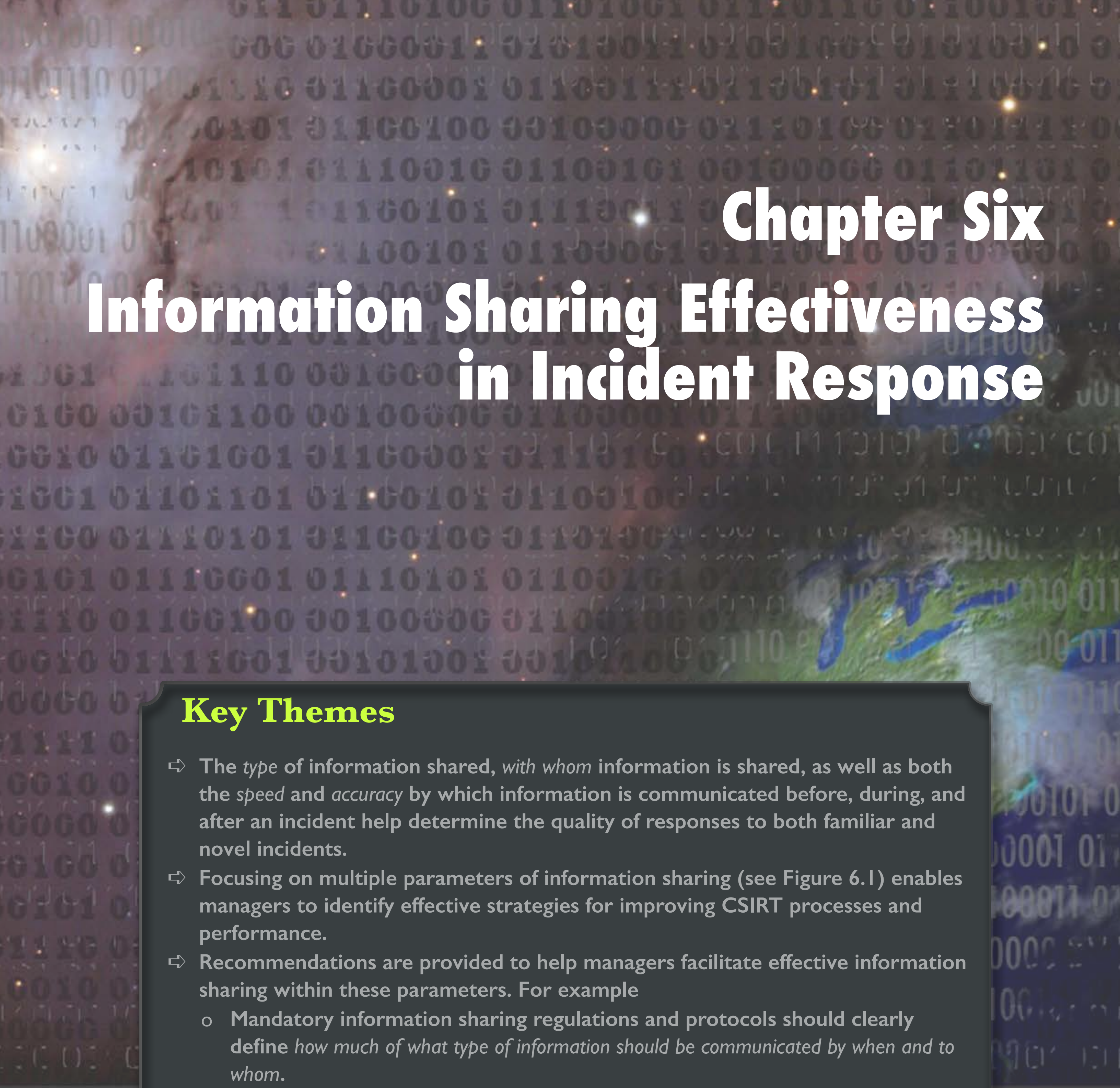
Tjaden, B., & & Floodeen, R. (2012). *Communication among incident responders – A study* (CMU/SEI-2012-TN-028). Software Engineering Institute, Carnegie Mellon University.

Wagner, C. (2004). Wiki: A technology for conversational knowledge management and group collaboration. *The Communications of the Association for Information Systems,* 13(1), 265-289.

Watson, W. E., Kumar, K., & Michaelsen, L. K. (1993). Cultural diversity's impact on interaction process and performance: Comparing homogeneous and diverse task groups. *Academy of Management Journal, 36*(3), 590-602.

Weick, K. E. (1990). Technology as equivoque: Sensemaking in new technologies. In P. S.Goodman & L. S.Sproull (Eds.), *Technology and organizations* (pp. 1–44). San Francisco: Jossey-Bass.

White, M. A., & Whitener, E. M. (1998). Mingle: A participative exercise to motivate the understanding of cross-cultural differences in international business. *Journal of Teaching in International Business*, *9*(3), 1-12.



Chapter Six

Information Sharing Effectiveness in Incident Response

Key Themes

- The *type* of information shared, *with whom* information is shared, as well as both the *speed* and *accuracy* by which information is communicated before, during, and after an incident help determine the quality of responses to both familiar and novel incidents.
- Focusing on multiple parameters of information sharing (see Figure 6.1) enables managers to identify effective strategies for improving CSIRT processes and performance.
- Recommendations are provided to help managers facilitate effective information sharing within these parameters. For example
  - Mandatory information sharing regulations and protocols should clearly define *how much of what type of information should be communicated by when and to whom.*
  - Managers should not discourage the discretionary sharing of information as such activities promote collaboration within and across teams and organizations.
  - Managers need to establish specific communication protocols based on the various levels of information sharing (e.g., two individuals, within team, intra- or inter-organizational); different strategies for improving information sharing might work at one level but not at another level.

Contents

6.0 Introduction

In the previous chapter, we covered some key parameters of effective communication and how managers can foster better communication in their teams. In this chapter, we cover in more detail the topic of cybersecurity information sharing. This topic has received considerable attention in the CSIRT literature and is at the core of effective incident response processes. Accordingly, in this chapter we provide additional coverage of this aspect of CSIRT communication.

Information sharing in the realm of cybersecurity reflects the exchange of cyber incident knowledge and threat data across and within organizations. Such information might include the identity of hackers and their known behaviors or skills, how a particular software program was infiltrated, or warnings about potential threats. The importance of information sharing has been recognized at the highest levels of national security and cyber defense (Alexander, 2012; "Cyber Security," 2015; Fowler, 2015; "The President Speaks about Cybersecurity," 2015). In recent years, discussions of information sharing in cybersecurity have focused heavily on exchanges of data between organizations (The White House, 2015; Hausken, 2007; Vazquez, Acosta, Brown, Reid, & Sprito, 2012). Specifically, President Obama's 2013 Executive Order "Improving Critical Infrastructure Cybersecurity" dedicates a section to increasing the "volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities" (Executive Order No. 13636, 2013, Sec. 4.a). In order to increase information sharing between entities, CSIRT managers will need to be aware of some unique issues that can make information sharing between entities challenging.

- **Barriers to sharing.** When incident response professionals at one organization discover an adversary uses specific techniques and tactics to infiltrate a system and then share that information with incident response professionals at other organizations, they help develop shared knowledge and understanding across all organizations that mitigates the potential for future attacks by that adversary. However, given the secrecy that exists between organizations, sharing details of how hackers gained intrusion into a company's system through a weakness might make the company appear negligent or weak. Companies are motivated to protect their reputations, and sharing information about a compromised system may put them in a vulnerable position.

  While organizations stand to benefit from learning about intrusions into other organizations, there is little motivation to share this information given the potential reputation damage it may cause. President Obama's 2013 Executive Order expanded the U.S. Government's voluntary information sharing program with the goal of increasing information sharing between "State, Local, Tribal, and Private Sector Entities" (Executive Order No. 13636, 2013, Sec. 4.a). A recent report from the Ponemon Institute that surveyed IT professionals in the U.S. and U.K. reported that 26% of participating organizations receive security threat-related information from other organizations but do not share such information with others, and 45% indicated their organization does not share with or receive security threat-related information from other organizations. These statistics suggest that organizations encounter multiple barriers to sharing cybersecurity information.
- **Liability**. Sharing information about intrusions may also come at a legal cost to organizations. If an organization voluntarily reports a cybersecurity threat or incident to an Information Sharing and Analysis Center (ISAC), and competitors are also members of the ISAC, the first company may open itself to a third party antitrust litigation. Alternatively, if an organization voluntarily reports a cybersecurity incident to a law enforcement agency, some situations may necessitate law enforcement requesting that the organization not share the information with an ISAC while the investigation is ongoing. While under such a gag order, the organization may be at risk of liability if other organizations are also harmed by the incident because they were not informed in a timely manner (Rosenzweig, 2012). The Poneman Institute's report also found that only 23% of respondents work in an incident response setting that has a public relations plan in place for the public sharing of information. This indicates that most organizations do not have a clear system or plan in place for handling the legal or public relations fallout that can exist.
- **Malicious sharing.** Competition between cybersecurity companies is tight and there have been claims of companies damaging their rivals by intentionally creating anti-virus software that identified benign files as malicious. For example, in 2015, the security company, Kaspersky Lab, was accused of targeting Microsoft Corporation and AVG Technologies, as well as other rivals, by reverse engineering competitors' virus detection software for the purpose of sabotage (Burlacu, 2015). Kaspersky denied that they injected false positives into cybersecurity virus aggregator websites and asserted that they believe trusted threat-data exchange is an important part of the cybersecurity ecosystem that should not be compromised (Coldewey, 2015). Menn (2015) argued that the proliferation of sharing between security companies has allowed for the rapid identification of new viruses and malicious content, but it has also created the sentiment that some firms are simply copying the work done by other security companies and passing it off as their own.

These CSIRT-specific issues illustrate the challenge of sharing information across organizational boundaries. Indeed, research indicates that many cybersecurity teams fail to optimally utilize information (Poneman Institute, 2014). Organizational scientists have noted such failings in other types of teams as well (Mesmer-Magnus & DeChurch, 2009; Stasser & Titus, 1985; Thomas &

McDaniel, 1990; Tiwana & Mclean, 2005). Many existing publications provide frameworks for sharing information in incident response scenarios, including the development of policies and standards, identification of what information should be shared, recommendations on how to keep the level of shared information scaled to current cyber-related events, and suggestions for what tools and technical programs may be particularly helpful (e.g., Fransen, Smulders, & Kerkdijk, 2015; Johnson, Badger, & Waltermire, 2014; Sandhu, Krishnan, & White, 2010; Vazquez, et al., 2012). However, information sharing in CSIRTs includes multiple parameters that should be considered, many of which are not covered in current manuals. In this chapter we provide a model of incident response information sharing that includes these parameters (see Figure 6.1). We also use the communication principles (i.e., relevance, quality, timeliness, frequency, information flow, and confirmation and response) from the previous chapter to provide suggestions to managers on how to improve CSIRT information sharing.

6.1 An Organizational Science Perspective on CSIRT Information Sharing

Information sharing in the realm of organizational science is described as "a central process through which team members collectively utilize their available informational resources" (Mesmer-Magnus, DeChurch, 2009, p. 535). This perspective considers aspects of cyber information sharing as more than the simple passing of detailed knowledge about security-related topics from one team or organization to another. It also includes more active forms of knowledge exchange among individual responders in teams, between teams, as well as across and between organizations. Knowing what kinds of information sharing should occur at each level during incident response, and adopting best practices for providing effective communication, can greatly enhance CSIRT effectiveness. Accordingly, in the next section of this chapter, we elaborate on three parameters of information sharing during cybersecurity incident response.

Knowing what kinds of information sharing should occur at what level during incident response, and adopting best practices for providing effective communication, can greatly enhance incident response effectiveness.

6.2 Elements of Information Sharing in CSIRTs

Figure 6.1 presents a model of cybersecurity information sharing that defines three distinct parameters: the *level* at which information sharing occurs, *process requirements* that influence how information is shared (e.g., policies and procedures), and the *degree of interaction* that occurs between all involved parties. Greater understanding by CSIRT managers about the impact of these parameters on information sharing can help them develop more efficient team processes.

6.2.1. EVIDENCE ON INFORMATION SHARING FROM OUR STUDY

The evidence for this model is based on a review of the CSIRT literature and on our analysis of 52 focus groups and interviews with approximately 150 participants from CSIRTs across the United States, the United Kingdom, Germany, Sweden, and the Netherlands. As part of our research effort, we constructed a multilevel taxonomy (i.e., classification system) of performance activities typically enacted by members of effective CSIRTs and multiteam systems (see Chapter 1, "Introduction to the Handbook," and Appendix A, "Taxonomy of Cybersecurity Multiteam System (MTS) Task Performance"). Twenty-eight of the 65 (42%) sets of incident response activities described in the taxonomy involve specific information sharing actions. Fourteen sets (21%) included team-level information sharing. Ten sets of activities in the taxonomy (15%) reflected information sharing between teams in CSIRTs. Our focus group interviews with CSIRT managers and analysts confirmed each of these 28 sets of information sharing activities as occurring in CSIRTs. These data support the distinctions among information sharing indicated in the model in Figure 6.1.

6.2.2 DEGREES OF INTERACTION BETWEEN INFORMATION SHARING PARTNERS

The first information sharing element in our model refers to the degree of interaction between CSIRT personnel involved during information sharing. Information sharing can entail a passive posting or distribution of information, a handoff of information from one individual or team to another, or an even more active and dynamic exchange of information entailing iterative offering of information and responding by multiple analysts (Ager, Johnson, & Kierman, 2006; Emerson, 1976).

Passive Information Sharing Between Partners

Passive informing occurs as a one-way generic distribution of information to others. The purposes of such information

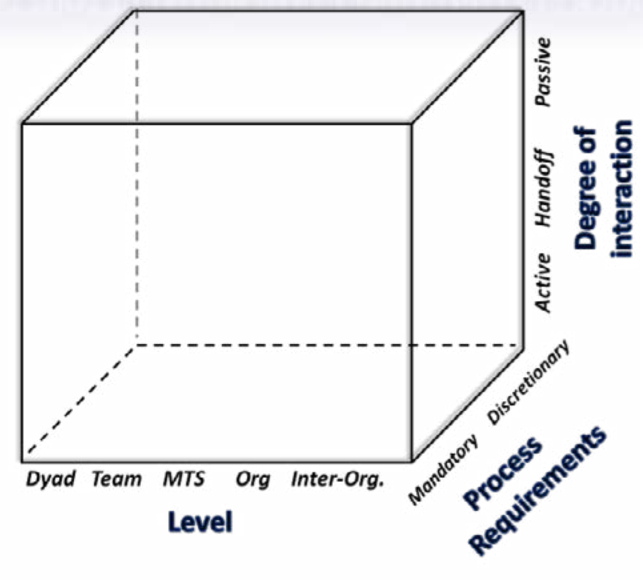


Figure 6.1 Cybersecurity Incident Response Information Sharing Model

sharing are (a) to keep others informed about potential trends, topics of interest, or general information that can be utilized in the future, and (b) to facilitate collective shared awareness and understanding among recipients. When incident response teams are under stress, passive communication tools have been found to be especially helpful for performance because they provide alternate ways for teams to maintain situational awareness with minimal effort (Strang et al., 2011). Examples of passive information sharing include:

- Utilizing a formal ticketing system to provide access to information that enables others to quickly and efficiently identify and mitigate threats based on previous work;
- Using tools such as wikis or virtual whiteboards to represent information in a pictorial format, which can increase the effectiveness of message delivery and retention (Strang et al., 2011); and
- Publishing fact sheets or white papers to provide insight about current issues and threats.

Information Sharing During Handoffs and Escalation

Handoffs entail more direct interaction with others than the passive one-way information sharing just described. Instead, handoffs from one individual or team to another occur with the implicit or explicit expectation that the recipient (i.e., the receiving analyst or team) will act on the information. Passive information sharing, in contrast, is simply sharing knowledge as a means of notification. Within this context, a handoff might be required based on a shift change, an analyst's level of experience, team or organizational functions, lack of resources or expertise, or incident severity. Examples of these circumstances include:

- A less experienced analyst passing incident-related information on to a more experienced analyst;
- A client handing over hard drives, images, and other media information to an incident response services team so their forensics team can conduct further analyses to investigate an incident;
- Sharing cyber threat signatures with anti-virus companies and other organizations with the expectation that they will include this information in product updates;
- A Federal agency requesting the services of a national, coordinating CSIRT during an investigation in a situation where the originating agency does not have the resources to independently analyze the incident.

> **“We have a wiki… it's our collaboration tool. Every single person on our team has full read/write access to it. This is the way documented knowledge is shared in the team. This is how we document that knowledge transfer is in the wiki.”**
>
> **~ CSIRT member**

In the previous chapter on communication processes in CSIRTs, we described the process of handoffs, along with the kinds of issues that can occur in such information sharing. We refer the reader to that chapter section (Section 5.3.2) for more information.

> **“[In] some cases we find there is evidence of a virus or worm or potentially malicious activity… and we are going to need to escalate… to our management, or to other teams in the organization … Our team is designed to be very tactical. We're going to respond to things more in the immediate term. If there's something that requires a lot of digging in… then we don't have the resources to handle that in our team. So, we're going to hand that off to an investigation team or a forensics team to do the kind of digging in that will be required for that.”**
>
> **~ CSIRT member**

Active Interaction between Information Sharing Partners

Active information sharing occurs when one party interacts directly and collaboratively with another to share information about a threat, vulnerability or attack. Such information sharing typically occurs before both parties engage in collective problem-solving around cyber incidents. This type of information sharing can occur, for example, when one analyst provides information to another, who, in turn, provides additional corroborating information. Recall from our description of communication processes in teams that different members might possess unique information based on their individual expertise, knowledge, or experiences (see Section 5.2.1; also see Chapter 7, "Collaborative Problem-Solving in Incident Response"). Active information sharing can entail the exchange of such information. Examples of active interactions between CSIRT professionals include:

- Incident briefings where one analyst presents specific incident-related information to the team and then other team members provide additional information to support those claims or expand the team's knowledge of the incident beyond what was previously known;
- Virtual interactions such as phone conferences and emails when CSIRT managers are checking on the status of an ongoing incident investigation;
- The continued exchange of information, in a back-and-forth manner between CSIRTs, related to incident mitigation in high profile cases that involve multiple teams and possibly organizations.

6.2.3 RECOMMENDATIONS FOR EFFECTIVE PASSIVE AND ACTIVE INFORMATION SHARING

Passive information sharing entails the posting or distribution of information without expecting a response. The key concern about such information exchange comes from a lack of confirmation and response, which can cause:

- *Decreased perceptions of relevant information* because sent information might not be fully relevant to the particular situations faced by potential receivers;
- *Failure to consider needs of the recipients* such as what information – and how much – they need;
- *Reduced information flow* because information posted passively might not target the right recipients.

> **"We really communicate a lot internally [in our] group and through email. Also, the members of the CSIRT team have started to communicate through their mailing list about what is going on."**
>
> **~ CSIRT member**

Thus, passive information sharing can result in the communication of information that is less relevant, complete, accurate, and less likely to go to the right people (see Chapter 5, "Communication Effectiveness in Incident Response," for additional descriptions of these communication parameters). To avoid such issues, managers should establish a communication protocol or a team charter (see Section 5.3.1) for passive information sharing that requires senders to do the following:

- Identify the recipients who would most benefit from or require the information being shared;
- Consider carefully what information – how much – these recipients need in order to accomplish their work;
- If time permits, have other CSIRT members who have similar information needs review the information posting for accuracy and completeness;
- When possible, use communication methods that allow confirmation of receipt to ensure information was received;
- Provide sender contact information, along with an invitation to request additional information if necessary.

Active information sharing involves reciprocal exchanges of information among individuals, teams, multiteam systems (MTSs), and organizations. Reciprocity can eliminate concerns with lower information relevance, quality, and information flow that can result from passive information sharing. However, active information sharing increases the overall frequency of communication. Accordingly, managers need to implement communication protocols that ensure such exchanges are kept short enough to confirm situational awareness, and information completeness, without unnecessary chatter.

6.2.4 INCIDENT RESPONSE PROCESS REQUIREMENTS

How and when information is shared can be either a function of established policies and requirements (e.g., rules, regulations) or entirely at the discretion of individuals, teams, MTSs, and organizations. Thus, information sharing in CSIRTs can reflect *mandatory* or *discretionary* exchanges of information.

Mandatory Information Sharing

Mandatory information sharing occurs when standard protocols require cybersecurity professionals to report specific types of data and information to others. These standards could stem from organizational policies and procedures, governmental regulations, rules from other regulatory agencies, or mandates from professional organizations. Examples of mandatory information sharing include:

- Mandatory reporting required of companies that participate in Information Sharing and Analysis Centers (ISACs) (Gal-Or & Ghose, 2004; Gal-Or & Ghose, 2005; Gordon, Loeb & Lucyshyn, 2003);
- United States federal agencies that are required to report incidents to US-CERT within specific time frames, as determined by incident category (West-Brown et al., 2003);
- Companies that contract with the government to provide critical infrastructure, or mission-critical national security capabilities, that may be required to share incident information with the government (Zheng & Lewis, 2015).

Discretionary Information Sharing

Discretionary information sharing occurs when an individual, team, MTS, or organization chooses to voluntarily exchange

> **[Agencies] have their own SOCs as well, and when they have an incident FIMSA requires that they report those incidents to US-CERT… that's part of a broader federal government reporting mechanism.**
>
> **~ CSIRT member**

knowledge and data about incidents with others. Discretionary information sharing might happen more often in some types of incident response settings than others. For example, in our research, we found that interactions within and across teams were more likely to be initiated during more severe events. Further, such information sharing could occur more often among individuals who have a preference for information sharing, or when a CSIRT leader outwardly encourages information sharing. Examples of discretionary information sharing related to cybersecurity include:

- Companies that choose to share information with federal agencies upon removal of personally identifiable information (PII; Zheng & Lewis, 2015);
- Decentralized or peer-to-peer information sharing relationships sponsored by specific industries (e.g., ISACs; Zheng & Lewis, 2015);
- Individual incident responders who contact a trusted cybersecurity colleague in another organization to informally discuss a new threat or vulnerability;
- Organizations that choose to share a threat-related experience, but not incident specifics, with another organization.

Several CSIRTs have existing policies regarding the classification of information. These policies often guide the voluntary versus required sharing of information. For example, Protected Critical Infrastructure Information (PCII) is a Department of Homeland Security program that allows for voluntary information sharing between private-sector critical infrastructure organizations and the U.S. government without fear of exposing sensitive or proprietary data (PCII Program, 2015). Additionally, many federal agencies use a "traffic light protocol" to indicate whether information should be shared or withheld. Thus, such a protocol could use a red, orange, green, and white color classification scheme to indicate how, when, where, and to whom information can be shared (US-CERT, n.d.).

6.2.5 RECOMMENDATIONS FOR EFFECTIVE MANDATORY AND DISCRETIONARY INFORMATION SHARING

Mandatory information sharing is typically defined by established policies, regulations, and rules. These regulations should clearly define *how much of what type of information should be communicated by when and to whom.* That is, regulations need to ensure the *relevance*, *quality*, *timeliness*, *frequency*, and correct *flow* of sent information. If managers receive reports that information being sent under specific rules is consistently incomplete, irrelevant, inaccurate, not timely, or sent too infrequently (or too frequently), then managers need to revise the regulations and protocols that determine the mandatory sharing of information. Moreover, when mandatory information sharing is also passive, managers need to also guard against the issues noted above under passive information sharing.

Discretionary information sharing occurs at the will of the sender. The primary communication issues that can occur with such information sharing are relevance, timeliness and frequency. Senders can choose to send all kinds of information to others, whether it is relevant or not. As such, they need to understand what information is necessary for recipients and limit communications accordingly. Also, the choice to send information needs to occur at the right time in the incident response cycle. Thus, senders need to be aware of when particular types of information are needed by others. Likewise, senders need to know how often such communication needs to happen. The primary purpose of information sharing is to promote situational awareness and provide sufficient knowledge for future action. Analysts choosing to send information at their discretion need to communicate no more than is necessary to accomplish these aims.

Managers should not discourage the discretionary sharing of information because such activities promote collaboration within and across teams and organizations. Thus, they need to set communication norms within their teams that support such information sharing. Accordingly, they need to establish communication protocols or team charters (see Chapter 5, "Communication Effectiveness in Incident Response," Section 5.3.1) as follows:

- Develop guidelines about what kinds of information are typically needed at different phases of most incident response cycles; responders should use these guidelines to determine when they should share particular kinds of information;
- Develop a shared understanding about when information becomes critical enough to share and what types of information are necessary to share during high impact events. Managers can do this by constructing different CSIRT and CSIRT MTS simulation scenarios and using them in guided discussions with the appropriate parties (see Chapter 5, Section 5.3.4);
- Determine how much information is needed to ensure

> **They are trying to get the vital sectors to tag along and be an intermediary between the knowledge that we are generating here internally and spread it out to our partners and the other way around. Our partners have valuable information that we might be able to share with other partners.**
>
> **~ CSIRT member**

situational awareness; limit communications to the point where situational awareness has occurred. Senders should request confirmation of received information.

6.2.6 INFORMATION SHARING AT VARIOUS LEVELS

The final element in this model, the *level* at which information sharing occurs, suggests that information can be exchanged between two individuals (i.e., dyadic sharing), within a specific team (e.g., a malware team), across different teams in an MTS (e.g., between watch and engineering teams), within a single organization (e.g., between a CSIRT and the CISO), or between organizations (e.g., between a private sector CSIRT and a national/coordinating CSIRT). One important consideration is that different strategies for improving information sharing in incident response might work at one level but not at another level. For example, posting a notice on a bulletin board might help individuals within a specific CSIRT become aware of important knowledge, but using the same method would not be as effective if that information needed to reach a large amount of individuals within another organization. Thus, employing a strategy to improve information sharing requires identifying at which levels such exchanges of information should occur.

Dyadic Information Sharing

At the dyadic level, information is shared between two people engaged in cybersecurity. These two people could be members of the same team, different teams, or from different organizations. Such information sharing can include:

- A member of the watch team shares information about an incident with a more experienced team member;
- Upon completing a shift, one analyst passes on incident-specific information to another analyst;
- A CSIRT MTS leader informs the organization's CEO that a security breach has occurred.

Within-team Information Sharing

At this level, information is shared and exchanged among multiple team members within the same team. Examples include:

- Team members possess different pieces of information all interact with the lead analyst assigned to a case to ensure he or she receives the necessary information to resolve an incident;
- Team members who share technical demonstrations of cybersecurity tools and techniques with all other members of their team;
- A CSIRT manager holds a team meeting to discuss new standard operating procedures.

Multiteam System Information Sharing

In MTSs, information sharing occurs between teams that work closely together. These exchanges can happen in several ways:

> **“One analyst will be responsible for looking at all the initial incidents as they come in, and that analyst will then pass to another analyst an event that needs to be looked at in more detail.”**
>
> **~ CSIRT member**

- Teams can designate specific members as a point-of-contact to share information with other teams (see Chapter 5, Section 5.3.7 on Boundary Spanning);
- Teams can hold meetings with other CSIRT teams (e.g., watch, incident response, threat intelligence, and malware and forensics teams) to gather and exchange information about the nature of a specific attack;
- Threat information gathered from different teams can be collated in a report to document various activities each team contributed to the incident response investigation.

> **“You end up having a lot of very good people with very good separate sources for information…If you get them together though, and really work with them, make it friendly, make sure you're including everybody in all of that, it really starts to work out.”**
>
> **~ CSIRT member**

Intra-Organizational Information Sharing

Information sharing within the organization occurs when CSIRT members inform their larger organization of incidents, policy changes, or other matters that affect the organization at large. Examples of such information sharing include:

- Communicating changes in login protocols to the entire organization;
- Informing all employees that an employee downloaded malware by opening a suspicious email attachment and communicating precautions to avoid additional compromise;
- Triaging an incident through interactions involving a range of individuals and departments.

> **“We come together every two months with all those teams [the policy team and the support team]. And we exchange information, sometimes, quite a lot, as a matter of fact.”**
>
> **~ CSIRT member**

Inter-Organizational Information Sharing

Information sharing in CSIRTs also occurs between different organizations. Sharing information at this level has received the most attention among cybersecurity professionals and is the target of many developmental frameworks that aim to enhance information sharing related to incident response (e.g., Johnson, Badger, & Waltermire, 2014; The White House, 2015). Examples of sharing information between organizations include:

- Publishing general alerts about specific threats to the public, to other organizations, or to other countries;
- CSIRTs working with law enforcement, legal, and/or other government agencies;
- Private sector CSIRTs exchanging information about threats, vulnerabilities, or attacks with other organizations;
- CSIRTs working with and attempting to share information within the same critical infrastructure sector, often through ISACs (e.g., Financial ISAC).

> **“When there is an incident, and if we have any doubt or need any advice, we always talk to each other. It depends, of course, on the classification of information… we use the traffic light protocol to decide what information can be disclosed within the organization.”**
>
> **~ CSIRT member**

6.2.7 RECOMMENDATIONS FOR EFFECTIVE INFORMATION SHARING AT VARIOUS LEVELS

Cybersecurity professionals can share information at multiple levels, from other individuals to other organizations. The primary communication issues that can occur with information sharing at different levels are *information flow*, *relevance*, *quality*, and *confirmation and response*. Certain information is more relevant for particular individuals, while other information needs to be shared with an entire team, MTS, organization, or even other organizations. Information that is shared with the entire team should be the kind of information that helps team members work together better. For example, when sending information to several analysts working on a joint problem, each analyst should receive all information that is relevant to that specific shared problem. Information shared across team boundaries should be the kind of information that helps multiple teams work together better. Likewise, only information that is necessary for an entire organization should be shared at the organizational level. Targeting the right information to the right level can facilitate communication relevance, quality and appropriate information flow.

When individual-to-individual information sharing occurs, confirmation and response is fairly straightforward. However, when an individual sends information to an entire team, MTS, organization, or to outside organizations, responsibility for confirmation and response might not be clear. The purpose of confirmation is to corroborate receipt of information and, more importantly, ensure that exchanged information is understood. In a team or a CSIRT MTS, many members can respond indicating different levels of understanding, or no one could respond because who is responsible for making confirmatory responses is not clear. The result can be confusion within the team or MTS.

> **“We want information coming in from organizations saying, ‘Okay, we're seeing this. We can provide that information to you. We've made an analysis. We made an assessment. Here have that.’ We want interaction. We're trying to develop something we call [name redacted for confidentiality], where we try to create a network of experts, an expert of organizations for information exchange.”**
>
> **~ CSIRT member**

To facilitate multi-level information sharing, managers need to establish communication protocols that do the following:

- Define what kinds of information need to be shared with an entire team, MTS, organization, or to external stakeholders.
- Develop a shared understanding of what information should go to which level. Managers can do this by developing different unit-specific simulation scenarios and using them in guided discussions with their unit. Such scenarios should focus on the information sharing relevance and quality at each level.
- Establish guidelines about which members within a team should respond to which kind of information sent to the entire team. Such responsibility might depend upon who has the lead on particular team-level problems. Also, on highly interactive team problems, these guidelines might require multiple team members to provide confirmatory and follow-up responses.
- Develop a shared understanding of different response protocols that depend upon different types of team problems. Managers can do this by developing different team-specific simulation scenarios and using them in guided discussions with their team.
- Establish *boundary spanners*, or individuals tasked with responding when information sharing occurs between teams in an MTS or between organizations. Managers should select those individuals who have particularly strong communication skills and social agility to represent their teams or CSIRT MTSs.

6.3 Summary

Note that many of the recommendations that managers should use to facilitate successful information sharing require ***the establishment of high quality communication protocols and the training of their teams to use these protocols.*** We refer readers to Chapter 5, “Communication Effectiveness in Incident Response” (Section 5.3.1), which describes team charters and some best practices on such protocols and training.

References

Ager, T., Johnson, C., & Kiernan, J. (2006, October). Policy-based management and sharing of sensitive information among government agencies. In *Military Communications Conference, 2006. MILCOM 2006. IEEE* (pp. 1-9). IEEE.

Alexander, K.B. (2012). An Introduction by General Alexander, *The Next Wave*, 19, (4) Retrieved from http://www.nsa.gov/research/tnw/tnw194/article2.shtml

Burlacu, A. (2015, August 15). Kaspersky lab denies creating fake malware data to sabotage rivals. Tech Times. Retrieved from http://www.techtimes.com/articles/76917/20150815/kaspersky-lab-denies-creating-fake-malware-data-to-sabotage-rivals.htm

Coldewey, D. (2015, August 14). Cybersecurity firm Kaspersky lab denies it sabotaged competitors. NBC News. Retrieved from http://www.nbcnews.com/tech/security/kaspersky-lab-denies-reports-it-sabotaged-competitors-n410206

Cyber Security: Preparing for and Responding to the Enduring Threat. (n.d.). Retrieved February 25, 2015, from http://www.fbi.gov/news/testimony/cyber-security-preparing-for-and-responding-to-the-enduring-threat

Emerson, R. M. (1976). Social exchange theory. *Annual Review of Sociology*, 2, 335-362.

Exec. Order No. 13636, 3 C.F.R. 11739-11744 (2013).

Fowler, P. X. (2015, February 18). Pass it On: New Executive Order Pushes Greater Sharing of Cyber-Threat Information [Web log comment]. Retrieved from http://www.swlaw.com/blog/data-security/2015/02/18/pass-it-around-new-executive-order-pushes-greater-sharing-of-cyber-threat-information/

Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. e & i *Elektrotechnik und Informationstechnik*, 132(2), 106-112.

Gal-Or, E. & Ghose, A. (2004). The economic consequences of sharing security information. In L. J. Camp & S. Lewis (Eds.), *Economics of information security* (pp.95–105). New York, NY: Springer.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research*, 16(2), 186-208.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, 22(6), 461-485.

Hausken, K. (2007). Information sharing among firms and cyber attacks.*Journal of Accounting and Public Policy*, 26(6), 639-688.

Johnson, C., Badger, L., & Waltermire, D. (2014). Guide to Cyber Threat Information Sharing (Draft). *NIST special publication*, 800-150.

Menn, J. (2015, August 13). Exclusive: Russian antivirus firm faked malware to harm rivals – Ex-employees. *Reuters*. Retrieved from mobile.reuters.com

Mesmer-Magnus, J. R., & DeChurch, L. A. (2009). Information sharing and team performance: A meta-analysis. *Journal of Applied Psychology*, 94(2), 535-546.

Ponemon Institute. (2014). Cyber security incident response: Are we as prepared as we think?. Retrieved from https://www.lancope.com/sites/default/files/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf

Protected Critical Infrastructure Information (PCII) Program. (2015, September21).RetrievedOctober12,2015,fromhttp://www.dhs.gov/protected-critical-infrastructure-information-pcii-program

Rosenzweig, P. (2013). *Cyber warfare: How conflicts in cyberspace are challenging America and changing the world*. Praeger, Denver, CO.

Sandhu, R., Krishnan, R., & White, G. B. (2010, October). Towards secure information sharing models for community cyber security. In *the 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)* (pp. 1-6). IEEE.

Stasser, G., & Titus, W. (1985). Pooling of unshared information in group decision making: Biased information sampling during discussion. *Journal of Personality and Social Psychology*, 48(6), 1467-1478.

Strang, A. J., Knott, B. A., Funke, G. J., Russell, S. M., Miller, B. T., Dukes, A. W., ... & Bolia, R. S. (2011). Collaboration technologies improve performance and communication in air battle management. *Military Psychology, 23*(4), 390-409.

The President Speaks About Cybersecurity. (2015, January 13). Retrieved from http://www.whitehouse.gov/photos-and-video/video/2015/01/13/president-speaks-about-cybersecurity

The White House. (2015). *Executive Order Promoting Private Sector Cybersecurity Information Sharing* [Fact sheet]. Retrieved from https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform

The White House, Office of the Press Secretary. (2015 February 13). Promoting private sector cybersecurity information sharing [Executive order]. Retrieved from https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

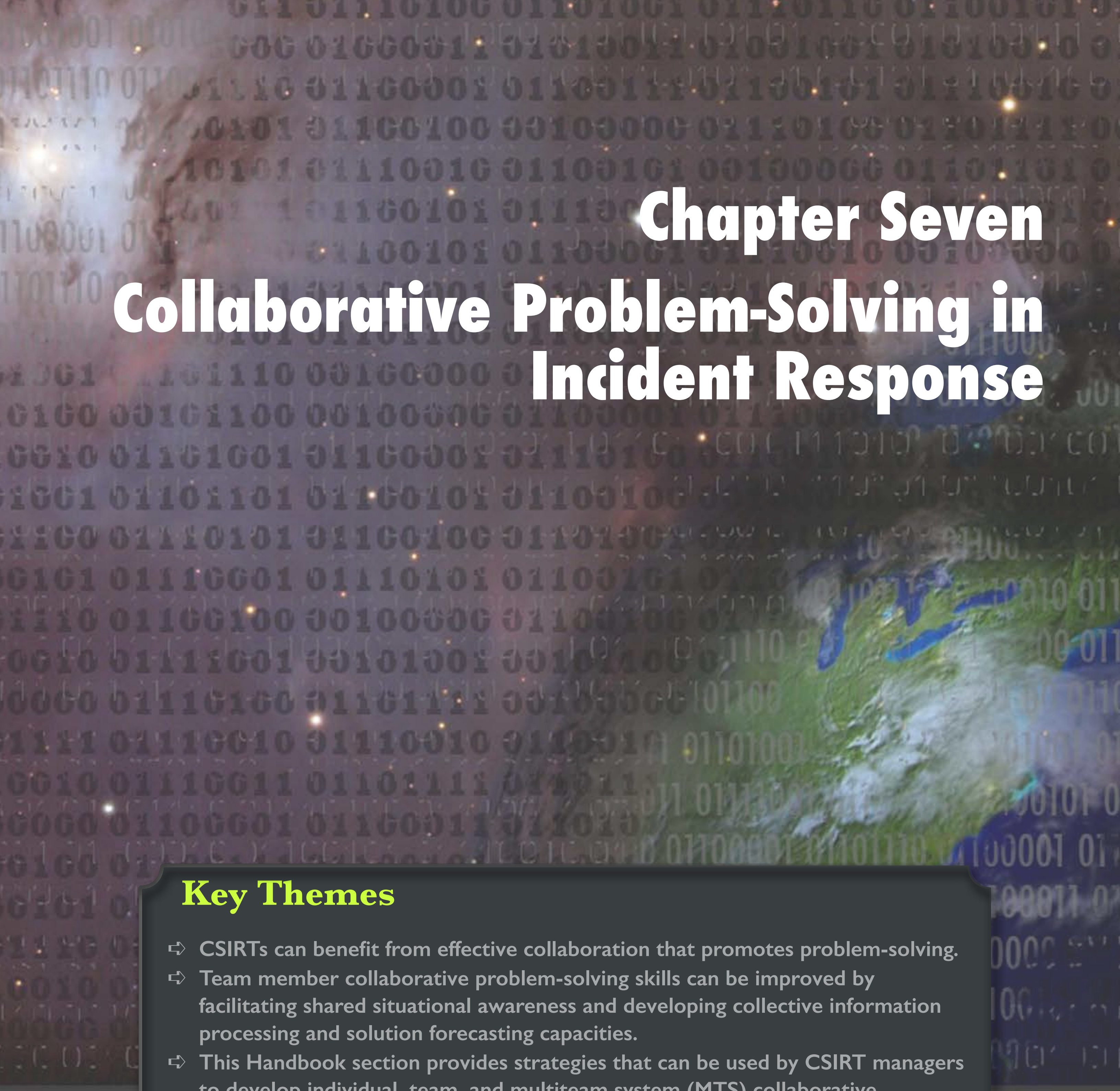
Thomas, J. B., & McDaniel, R. R. (1990). Interpreting strategic issues: Effects of strategy and the information-processing structure of top management teams. *Academy of Management Journal*, 33(2), 286-306.

Tiwana, A., & Mclean, E. R. (2005). Expertise integration and creativity in information systems development. *Journal of Management Information Systems, 22*(1), 13-43.

Vázquez, D. F., Acosta, O. P., Brown, S., Reid, E., & Spirito, C. (2012, June). Conceptual framework for cyber defense information sharing within trust relationships. In *4th international conference on cyber conflict (CYCON)* (pp. 1-17). IEEE.

West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., & Ruefle, R. (2003). Handbook for computer security incident response teams (CSIRTs) (No. CMU/SEI-2003-HB-002). Carnegie-Mellon University, Pittsburgh, PA. Software Engineering Institute.

Zheng D. E., & Lewis J. A. (2015). Cyber Threat Information Sharing: Recommendations for Congress and the Administration. Center for Strategic & International Studies, Washington, DC.



Chapter Seven

Collaborative Problem-Solving in Incident Response

Key Themes

- CSIRTs can benefit from effective collaboration that promotes problem-solving.
- Team member collaborative problem-solving skills can be improved by facilitating shared situational awareness and developing collective information processing and solution forecasting capacities.
- This Handbook section provides strategies that can be used by CSIRT managers to develop individual, team, and multiteam system (MTS) collaborative problem-solving skills.

Contents

7.0 Introduction

The nature of CSIRT work is, at its core, problem-solving. When an event is detected, an analyst must determine its nature and parameters, forecast the threat it can pose, and generate a resolution strategy. When events are novel and/or turn out to be high-severity incidents, multiple analysts and teams will likely work together to understand its parameters and to develop, evaluate, and implement solutions. As responding to incidents can be fast-paced, requiring rapid solutions, effective CSIRTs learn to integrate the contributions of different analysts quickly in the process of incident resolution. They know who has what expertise that pertains to a particular problem. They also trust one another to offer good ideas and follow through on solution commitments. In other words, members of effective CSIRTs are excellent collaborative problem-solvers.

> **“There are a lot of times where collaboration is necessary… There are incidents or technical problems maybe that require you to consult someone else who might have more knowledge or has a different perspective.”**
>
> **~CSIRT Leader**

This chapter and the following two chapters cover different aspects of *collaborative problem-solving* in cybersecurity incident response. In this chapter, we describe the steps in the process of collaborative problem-solving. We also describe adaptive thinking as a part of this process. Because each of the following two topics is particularly vital to effective collaborative problem-solving, in the next two chapters we discuss separately:

- Shared knowledge of unique expertise, which contributes to effective collaborative problem-solving; and
- Trust as a necessary component of collaborative problem-solving.

> **“So that especially in the bigger incidents..., there [are several] people, there's an incident manager and there [are] people with different roles, then you sit together and say okay, time out; what has happened, and what are our next steps?”**
>
> **~CSIRT Member**

When CSIRT members need to collaborate to resolve incidents, there are specific collaborative problem solving techniques they can use to reach effective solutions quickly. In this chapter, and in the following two chapters, we will offer strategies that managers can use to improve a CSIRT's use of these techniques.

7.1 Assessing Collaborative Problem-Solving Capacity

The following assessment exercise is designed to provide managers with a diagnostic tool in order to determine how well the how well the CSIRT, individuals, or component teams within the CSIRT MTS collaborate to solve problems. This will ultimately help determine the social maturity of the CSIRT (See Chapter 2, “The Social Maturity of CSIRTs and Multiteam Systems,” for additional information). Based on the responses to this assessment

ASSESSMENT EXERCISE

1. Team members in my CSIRT proactively solicit help from each other.
2. My team members get together to brainstorm and to consult each other about incident resolution.
3. My team members use the knowledge they have gained from other team members in resolving a novel incident.
4. My team members work together to determine the potential consequences of an event or threat to the cybersecurity of the organization or to constituents.
5. Members of my CSIRT consider multiple viewpoints when resolving an incident.
6. Members of my CSIRT are willing to switch to new kinds of solutions when existing ones may not be the best.
7. Members of my CSIRT try new ways of thinking about novel events and incidents.
8. Members of my CSIRT adopt new ways of resolving incidents.
9. Members of my CSIRT are comfortable deviating from normal or typical ways of resolving incidents.
10. My team members change their behaviors or protocols as a result of previous incidents.
11. Members of my team are likely to try new ideas and solutions when resolving incidents.
12. My team members incorporate the expertise of other teams into incident resolution.
13. Teams in my CSIRT proactively solicit help from other teams.
14. Multiple teams get together to brainstorm and to consult each other about incident resolution.
15. Multiple teams work together to determine the potential consequences of an event or threat to the cybersecurity of the organization or to constituents.
16. Teams in the CSIRT MTS change their ways of interacting with one another as a result of previous incidents.

exercise, managers can determine whether they would benefit from the strategies offered in this chapter. Managers should consider the time and resources required to implement these strategies relative to their need for improvement.

TABLE 7.1 COLLABORATIVE PROBLEM-SOLVING PROCESS MODEL

COLLABORATIVE PROBLEM-SOLVING STEP	PROBLEM-SOLVING STEPS IN CSIRTS
1. Problem Definition and Information Gathering	Understand the nature of an incident by examining the available information and defining the type and severity of an incident. • Prepare incident ticket; determine triage requirements; forecast potential damage; gather and examine incident evidence
2. Information Organization and Knowledge Integration	Compare the incident to existing knowledge within the CSIRT to determine what experience will be helpful with incident resolution. • Exchange information about the incident among members of the CSIRT; determine what relevant knowledge or experience exists in the CSIRT
3. Idea Generation and Evaluation	Discuss possible steps for incident mitigation and determine which ones are likely to be the most effective. • Generate and define possible solutions; determine likely solution effectiveness
4. Implementation Planning	Actively plan for incident resolution by developing and evaluating the best fitting solution based on the results of the idea generation and evaluation phase. • Develop implementation plan; determine CSIRT member involvement in solution implementation; modify plan if required
5. Solution Monitoring	Determine if solution implementation is effectively mitigating the incident. Adjust the plan as required. • Mitigate incident by using tools, applications, or procedures as specified by the implementation plan

Note. Derived from Mumford, Medeiros, and Partlow (2012)

Assess how your CSIRT is functioning in this area by responding to the above assessment using a 1-5 scale where 1= Strongly Disagree, 2= Disagree, 3= Neither Agree nor Disagree, 4= Agree, 5= Strongly Agree.

GO TO PAGE 128 FOR
STRATEGIES FOR CSIRT MANAGERS

7.2. Background

Research has identified a consistent process that teams use for effectively solving novel problems. Collaborative problem solving occurs in a series of steps, beginning with problem identification and ending with solution implementation and monitoring (Mumford, Medeiros, & Partlow, 2012; Mumford, Mobley, Reiter-Palmon, Uhlman & Doares, 1991). CSIRTs mirror these processes when they work together to resolve incidents. Table 7.1 presents a modified version of these steps with the addition of sample collaborative incident response activities. While these sample activities represent typical actions, other processes might certainly occur within each step. These steps may also occur between multiple teams in the CSIRT.

Understanding these steps will enable CSIRT managers to guide more efficient within and between team collaborative problem solving.

7.2.1 COLLABORATIVE PROBLEM-SOLVING PROCESSES

When incidents involve collaboration between multiple team members, the team members:

- Exchange ideas and determine the nature and parameters of an emerging incident or threat;
- Brainstorm and build upon each other's ideas for resolving the incident or threat;
- Collectively evaluate possible threat resolutions;
- Choose the best incident mitigation solution; and
- Determine the steps needed to implement the chosen solution (Fiore, Smith-Jentsch, Salas, Warner, & Letsky, 2010; Zaccaro, Hargrove, Chen, Repchick, & McCausland, 2016).

These behaviors are detailed in the *Taxonomy of Cybersecurity Incident Response Performance* in Appendix A. Note that these behaviors occur within incident response teams, as well as between teams in a CSIRT MTS.

> **“Well, today I'm working on something –[where] we're seeing alerts for certain traffic. I'm trying to figure out, you know, why it's happening, whether… something [is] compromised on our network or whether it's something outside. I hit a dead end; so I sent out an email to the whole team to see, you know, 'Hey, can anyone else provide me any information? Have you seen this before?'”**
>
> **~CSIRT Member**

> **But if somebody in critical infrastructure says, hey, I have this question or we have had this kind of incident or whatever, so that's information we can take back and we can use it for our situational awareness, that's where we start.**
>
> **~CSIRT Member**

In general, the problem-solving processes in Table 7.1 are effectively accomplished by three main processes that CSIRT leaders can target when developing training or strategies to improve CSIRT performance. They include (1) *shared situational awareness*, (2) *collective information processing*, and (3) *solution forecasting*.

Shared Situational Awareness

The resolution of an incident by an individual team or CSIRT MTS begins with developing a shared awareness of an event and the threat it may pose. This requires collective thinking in three ways (Endsley, 1995):

1. Detecting key elements of a developing event;
2. Interpreting and comprehending the information about the event in order to determine if it poses a threat; and
3. Forecasting the possible implications of such a threat to networks and information systems.

These collective procedures also reflect the crucial elements of the first two steps in the collaborative problem-solving model in Table 7.1. Detecting key event details requires systematic information gathering (Mumford, Mecca, & Watts, 2015). To accomplish this, multiple team members with differing sets of expertise may search for, gather, and share different pieces of the puzzle, increasing the likelihood of generating a complete picture of the event. Such information searching and gathering may also occur between teams in a CSIRT MTS.

> **If I want to work with another person on the tier two team, what I will do is I'll look at an alert, I'll do all the analysis I can do. And then I'll take a person from my team and say, hey, here's what I think happened, here's the general overview of what I've found so far. What do you think from looking at it? And I'll take that person's interpretation, you know, maybe they're seeing things that I didn't notice, or they say, oh, well, you saw that and you thought it was this. But really I think it was this. And then based on our collaboration, you know, we'll make a determination to say with medium, low or high confidence we think that this happened.**
>
> **~CSIRT Member**

Members with different expertise can combine their knowledge to develop a broader and deeper understanding of events, and they can determine different ways particular incidents threaten a system. The result is a more thorough shared understanding of a possible threat, which can then be used to determine the necessary elements of an appropriate solution for specific incidents (Mumford et al., 2015). Thus, developing shared situational awareness is necessary for the other steps in the collaborative problem-solving to be accomplished effectively.

> **You write it in the report and everybody reads the reports within the next few days. We can chime in and reply to the report and say, 'Hey, I saw that,' or, 'You're being too strict on this.'**
>
> **~CSIRT Member**

Collective Information Processing

Collective information processing occurs when individual team members share their ideas, thoughts, and suggestions with others on the team (Steps 2 and 3 in Table 7.1; Clark & Chalmers, 1998). Such collaboration also happens among members from different teams in a CSIRT MTS. For example, one member of the CSIRT can share his or her thoughts on a particular incident in conversation with another CSIRT member. That other CSIRT member may build on the observations of the first team member by offering additional ideas or suggestions based on his or her own unique expertise and experience. As collaboration expands to include more CSIRT members, the cycle of knowledge sharing potentially continues until an entire team or multiple teams have been involved in the process or until the problem has been resolved. Further, in mature CSIRTs, members feel comfortable critiquing and challenging one another's ideas, which, in turn, produces even stronger ideas (Edmondson & Lei, 2014). This collaborative thinking, then, fosters a more effective idea generation and evaluation process, becoming the basis for successful solution generation and evaluation. At this point, another collaborative process can occur – solution forecasting.

Collective Solution Forecasting

Collective solution forecasting refers to the prediction of possible outcomes and consequences arising from various possible actions (Bryne, Shipman, & Mumford, 2010; Mumford, Lonergan, & Scott, 2002; Rouse & Morris, 1986). It involves "a process of mentally simulating imagined future scenarios or events. It is used by decision makers to anticipate potential obstacles and hindrances, or to play out a course of action and evaluate its potential for success" (Adis, 2013, p. 3). Solution forecasting occurs during steps 3, 4 and 5 in Table 7.1. In collective solution forecasting, CSIRT members work together to discuss possible outcomes of handling incidents in various ways.

The value of conducting such forecasting as a team is that different members may have different experiences and insights on the various consequences of potential solutions. They bring different perspectives to solution considerations. In a CSIRT, the process of collective solution forecasting benefits from engaging a broader range of stakeholders in the solution consideration process. Different teams bring their own issues and needs to the discussion and ensure that incident resolution strategies account for the widest range of possible concerns.

Summary: Challenges for CSIRT Managers

These three processes of shared situational awareness, collective information processing, and collective solution forecasting contribute to effective CSIRT problem-solving. For CSIRT managers, *the critical tasks involve creating the right conditions for teams and MTSs to share ideas and work together to generate and implement the right solutions.* Members bring different experiences and expertise to collaborative problem-solving. Managers need to make sure that all team members know who has what knowledge and expertise within and across their CSIRT, so analysts can call on the most knowledgeable person quickly at different stages of problem-solving. In other words, they need to help their teams acquire a shared knowledge of unique expertise (SKUE). Chapter 8 ("Shared Knowledge of Unique Expertise") provides strategies for managers to help their teams acquire SKUE.

Another key concern for CSIRT managers is to make sure that CSIRT members have the high levels of trust necessary to engage in collaborative problem-solving both within and across component teams. Offering new ideas, especially about novel kinds of threats, can be intimidating for some analysts, especially in teams with competitive or distrusting climates. Managers need to establish a "psychologically safe" place for members to offer unusual ideas. Effective incident response depends upon members evaluating and critiquing one another's ideas; this cannot happen unless members know that such evaluations are well-intentioned--and intended to produce the best solution for everyone. Chapter 9 ("Trust in Teams and Incident Response Multiteam Syetems") discusses strategies for how managers can establish the levels of trust necessary for effective collaborative problem-solving.

7.2.2. ADAPTIVE PROBLEM-SOLVING IN CSIRTS

To be effective, CSIRTs are required to be adaptive. Hackers respond to countermeasures by coming up with new and different ways to attack systems. This means that analysts and incident responders often face novel incidents and new types of cybersecurity problems. Organizational scientists have also noted that adaptation is required when teams and individuals are working under stress, handling crisis or emergency situations, working with individuals and teams from other cultures, and learning new technologies (Pulakos, Arad, Donovan, & Plamondon, 2000).

Despite this need for adaptation, CSIRTs and teams often respond to new challenges with the same habits, routines, or solutions. Successful adaption requires individuals and CSIRTs to make fundamental changes in thinking and behavior in response to changing events (Baard, Rench, & Koslowski, 2014). Most people use the same frame of reference or perspective to address an incident or solve a problem even when the underlying nature of the problem has fundamentally changed (DeYoung, Flanders, & Peterson, 2008; Zyphur, 2009). Managers can counteract this tendency by using the following prompts when their teams are engaged in collaborative problem-solving:

- What is a different way of thinking about this problem?
- What other possible solutions might apply to this problem?
- What happens if this solution is wrong (contingency thinking)?

These and similar kinds of cognitive *frame-changing* prompts help analysts and teams adapt how they are thinking about a new type of problem and use different perspectives when deriving appropriate solutions (DeYoung et al., 2008; Hong, Morris, Chiu, & Benet-Martinez, 2000).

Adaptive thinking can also be encouraged and developed by (a) facilitating contingency planning in pre-briefing sessions, and (b) using exploratory learning approaches that include a wide variety of practice scenarios. Such practice variety helps individuals and teams become more comfortable with the process of changing the ways they think about and adapt to different types of incidents and problems (Nelson, Zaccaro, & Herman, 2010). The section below on strategies for enhancing collaborative problem-solving contains additional information on contingency planning (Strategy 1) and use of active learning with frame-changing prompts (Strategy 4).

7.3 Project Findings

Our project found evidence that effective CSIRTs engage in each of the collaborative problem-solving steps discussed above when reacting to an identified threat. Table 7.2 summarizes data from our focus groups with CSIRTs indicating how many times a particular step was said to be important for CSIRT effectiveness. Of note is that these specific problem-solving behaviors were important for team-level effectiveness and MTS-level effectiveness (problem-solving between multiple teams).

We also found that CSIRTs often *proactively* engage in several of these steps at the team and MTS levels. Instead of reacting to a threat that has been identified, CSIRTs collectively try to develop solutions that will prevent attacks. Table 7.3 shows some of the steps that CSIRTs indicated were important.

These two tables reflect the identification of these proactive and reactive problem-solving behaviors by CSIRT managers and analysts as being important to team and MTS effectiveness in CSIRTs. The consistently higher percentage of collaborative problem solving steps being mentioned as important in MTS (or between-team) effectiveness versus within-team effectiveness supports our broader research finding that CSIRTs are primarily MTSs, conducting problem-solving as closely-knit interdependent teams.

Our survey of 88 CSIRT professionals regarding critical knowledge, skills, abilities and other attributes that contribute to effective incident response (see Chapter 1, "Introduction to the Handbook")

TABLE 7.2 CSIRT *REACTIVE* PROBLEM-SOLVING BEHAVIORS FROM OUR FOCUS GROUPS AND INTERVIEWS

CSIRT PROBLEM-SOLVING STEP	EXAMPLE BEHAVIORS	% OF INTERVIEWS WHERE THIS STEP WAS SAID TO BE IMPORTANT FOR TEAM EFFECTIVENESS (N= 43)	% OF INTERVIEWS WHERE THIS STEP WAS SAID TO BE IMPORTANT FOR MTS EFFECTIVENESS (N=43)
Detect and gather information about security incidents	Collectively focus team attention on intrusion detection alerts; exchange information and ideas with other team members about nature of attack	49%	58%
Triage (assess, categorize, and prioritize) incoming incident(s)	Exchange information and reach agreement across affected component teams about problem parameters posed by the nature of the event	65%	81%
Develop a comprehensive mitigation solution	Exchange ideas among component teams about potential solutions; reach consensus on a best-fitting solution	42%	60%
Implement comprehensive mitigation solution	Coordinate across component teams in executing implementation of selected security solutions	42%	65%

TABLE 7.3 CSIRT *PROACTIVE* PROBLEM-SOLVING STEPS AND FOCUS GROUP SUPPORT

CSIRT PROBLEM-SOLVING STEP	EXAMPLE BEHAVIORS	% OF INTERVIEWS WHERE THIS STEP WAS SAID TO BE IMPORTANT FOR TEAM EFFECTIVENESS (N=43)	% OF INTERVIEWS WHERE THIS STEP WAS SAID TO BE IMPORTANT FOR MTS EFFECTIVENESS (N=43)
Determine necessary security tools, applications, and infrastructure	Generate and evaluate members' ideas and proposals about necessary, viable, and innovative security measures, tools, and applications	30%	40%
Set-up selected security tools, applications, and infrastructure	Coordinate implementation of security measures, tools, and applications across team members to ensure the most appropriate system configuration	30%	42%

indicated two problem-solving skills were in the top 10 highest rated attributes:

1. Skill in reviewing related information to develop and implement solutions to complex problems (5th highest)
2. Skill in working with other members to solve problems and come to solutions that will help the team (10th highest)

These data indicate the necessity for CSIRT managers to ensure that their teams can collaborate well as an MTS and work together to solve incident-related problems.

7.4 Improving CSIRT Collaborative Problem-Solving

In this section, we provide exercises and recommendations related to effective problem-solving. These exercises and recommendations are based on the background information and findings of our project team described in the previous section. Please use the assessment exercise at the beginning of this chapter to evaluate the effectiveness of collaborative problem-solving in your team or CSIRT and to help you determine the best strategies to improve your team.

The most common method for training team problem-solving skills is simulation-based training (SBT). Chapter 5 ("Communication Effectiveness in Incident Response") described a generic simulation-based training format. SBT simulates a crisis or high-pressure incident that team members must work together to solve. Such training can also be formatted to include multiple teams coordinating in a CSIRT MTS. Team members (or

> **"And we involve people from other teams to provide information to help us with incident analysis, or deal with technical – in-depth description of a technical issue. So yes, we involve them, and also the other way around. If there's a big incident, we could be providing an analyst or an advisor to be on the team."**
>
> **~CSIRT Member**

multiple teams) that are geographically dispersed can coordinate their activities during SBT if virtual communication methods are available. One general example of a SBT format is Distributed Dynamic Decision-making (DDD; Ellis, Bell, Ployhart, Hollenbeck & Ilgen, 2005), which can be used for several different scenarios. For example, a humanitarian relief effort was simulated through DDD where team members needed to get supplies to refugees while defending them from hostile attacks. These requirements can be easily adapted to a CSIRT context. Simulation training should have the following properties to be effective (Alison, et al., 2013; Oser, Gualtieri, Cannon-Bowers & Salas, 1999):

- Realism:
  - o Make the incident as close to a real incident as possible by re-creating an incident that already happened or is likely to happen.
- Appropriateness of Scenario:
  - o Base scenarios on critical incidents or trigger events that require use of the team attributes you are trying to build.
- Immersion:
  - o Make the exercise as engaging as possible for teams by requiring constant activity (e.g., they must monitor multiple systems).
- Performance Assessment:
  - o Build in a method of performance assessment by requiring teams to present their solutions, using measurable data from the team's actions (e.g., time taken to detect a problem), or having observers check off and rate team behaviors.
- Feedback Provision:
  - o Based on these and other performance measures, focus feedback on how the team should work together to respond to the scenario. Note: Team feedback should be given to the team as a whole, but individual feedback should be given to each team member in private (Koles, 2001).

To reduce costs associated with SBTs, CSIRTs can build on existing simulations or related training strategies already in use. Several CSIRTs employ strategies such as black hat, red teaming and specific training simulations like Tracer FIRE for incident coordination and other CSIRT-related topics (http://csr.lanl.gov/tf/). In Tracer FIRE, an experienced CSIRT member creates an incident simulation based on an actual or fictional incident that happened or could happen within an organization. All of the training exercises are applied to the incident, and the team tries to find bits of information to tie together, define the problem, and create a solution. In this section, we offer several strategies that can either be implemented through SBT (new or already existing programs) or adopted on their own as strategies to improve collaborative problem-solving within and between teams. We focus mainly on aspects of simulation training that have been shown to effectively improve collaborative problem-solving: pre-briefing and debriefing. While these strategies may seem obvious, we explain the principles that must be followed to make them effective.

Pre-mission planning, also called pre-briefing, targets phases of the problem-solving process that involve definition of the problem and shared awareness of the problem.

7.4.1 STRATEGY 1: ENGAGE IN PRE-MISSION PLANNING (OR "PRE-BRIEFING")

Pre-mission planning, also called pre-briefing (see also Chapter 5: "Communication Effectiveness in Incident Response"), targets phases of the problem-solving process in Table 7.1 that involve definition of the problem and shared awareness of the problem. CSIRT members cannot resolve an incident if they cannot define the problem parameters. Teams (and MTSs) who engage in pre-briefing create a problem-model (Orasanu, 1994), which is essentially a framework for dealing with an incident before the CSIRT takes any type of action. Such models include a shared understanding of the problem, its causes, and potential solution parameters.

Pre-briefing serves to map out or document the results of the problem-solving process so that individual members can contribute to resolution without confusion or process loss.

Recommendations for use:

Creating a pre-briefing guide for problem-solving and incident resolution will ultimately lead to better solutions and quicker response time. If CSIRT members share awareness of the situation, they can find and implement a solution with fewer negative consequences more quickly. In a simulation, facilitators or managers can train teams on how to effectively engage in pre-briefing and allow them to practice in an incident scenario. Managers and leaders should determine the most important features of the pre-briefing before the team engages in problem-solving (Bolstad, Endsley, Costello & Howell, 2010) based on the teams and/or team members involved in responding to an incident.

There are a number of planning tools that can be used to guide pre-briefing. Sparks (2015) presented a planning and debriefing guide that has been used for cybersecurity incident response in the United States Air Force. An explanation of this guide can be found at https://www.first.org/conference/2015/program#peffective-team-leadership-and-process-improvement-for-network-security-operators.

One tool used in simulations to facilitate pre-planning is a virtual whiteboard for team members who are geographically dispersed. With this tool, all team members can see a map of the simulated environment and make related notes on it (similar to information boards used to facilitate SKUE--see Chapter 8, "Shared Knowledge of Unique

Expertise"; Miller, Price, Entin, Rubineau, & Elliott, 2001). A process or mission map allows teams to map out their plan according to the problem phases, along with strategies for completing these phases (Stout, Cannon-Bowers, Salas, & Milanovich,1999). For example, when an analyst suspects an intrusion, the team might go through several checks to determine where the intrusion happened and which systems are affected. A process map allows the team to indicate which systems need to be checked, who will check them, and what to check for. With these tools, all team members can share knowledge related to the incident environment and their strategy going forward (see Strategy 2). The virtual whiteboard allows for integration of team members' unique information related to a particular incident, which builds new knowledge. When team members all contribute their unique information (see Strategy 2), information can be integrated to create new knowledge, improve situational awareness among team members, and increase shared understanding of the problem/incident. This also corresponds to steps 2 and 3 of the problem-solving model. Managers and facilitators can provide feedback and guide team members how to effectively implement and use these tools during SBT.

Steps to Implement Pre-Briefing Strategy

CSIRT managers can use the following steps to implement a pre-briefing strategy (please refer to Sparks (2015) as an example of a pre-briefing approach with CSIRTs):

1. Determine the kinds of incidents for which you would implement pre-briefing.

Not all types of incidents require an elaborated pre-briefing process. Generally, pre-briefing should be used for events that (a) are higher in severity levels, and (b) require higher levels of collaboration among members of the CSIRT or with other teams in a CSIRT MTS.

2. Develop an action plan for incident resolution.

This plan should include:

- The end-state objectives
- The key tasks that should be accomplished
- The key members/analysts who will be collaborating to resolve the incident
- The roles each member will assume in incident resolution
- How and when specific interactions among analysts need to happen
- Communication protocols
- The expected timeline of task accomplishment and incident resolution

3. Brief the action plan to the rest of the CSIRT.

Managers need to provide the action plan to the team in a succinct but thorough manner. In this briefing, they should:

- Provide details of the action plan
- Indicate how the team will track and assess progress throughout the plan
- Define key roles and responsibilities
- Define key assumptions and the manager's intent regarding how an incident should be resolved

4. Ensure that all team members understand the proposed plan.

- Conduct "verbal rehearsal" of the plan by having members indicate how they will accomplish their parts of planned interactions
- Provide a "psychologically safe" climate for members to ask questions about aspects of the plan (see Chapter 9, "Trust in Teams and Incident Response Multiteam Systems")

5. Engage in contingency planning (see below: "Contingency Planning: A Variation of Pre-briefing").

- Have team members determine possible obstacles that could impede them from completing their assigned tasks
- Then, have members consider contingent strategies for avoiding or removing these obstacles
- Team members can also engage in a "premortem" exercise (See Chapter 4, "Decision Making in CSIRTs, Strategy 3). To do this exercise, they are asked to think about the following:
  - Imagine that you have already responded to the incident and failed
  - Provide reasons why you might have failed

The premortem exercise can reduce the possibility of overconfidence and confirmation bias in teams.

Effectiveness Evidence:

Pre-briefing tools have been shown to lead to effective problem-solving outcomes. Teams using virtual whiteboards have engaged in 6% more collaborative planning behaviors with greater accuracy in defining the problem (Miller et al., 2001). Correct diagnosis of a problem has significant implications for creating solutions and the effectiveness of those solutions. Teams that use mission and process maps to strategize in advance of incident coordination have seen 59% better shared awareness of the problem among team members (Stout et al., 1999). Specifically, they had a shared understanding of the information other team members would need during incident coordination (Stout et al., 1999; see Chapter 8, "Shared Knowledge of Unique Expertise," for more on this process).This shared awareness allowed members to anticipate others' needs more easily. Teams that engaged in high-quality pre-briefing in high workload environments provided 70% more information to teammates in advance, thus decreasing resolution time (Stout et al., 1999). Teams that engaged in higher quality planning also saw between 28% and 44% fewer errors during periods of higher workload (Stout et al., 1999). Teams anticipating one another's informational needs made 30-43% fewer errors during high workload periods (Stout et al., 1999).

Managers can increase effectiveness of pre-briefing tools by using prompts. Teams who were prompted by managers to engage in knowledge integration behaviors using a virtual whiteboard shared significantly more unique information than teams who were unprompted (68%). They also demonstrated 12% higher cognitive congruence, which means that they shared an awareness of the most important pieces of information that they used when constructing their plan (Rentsch, Delise, Mello & Staniewicz, 2014). These findings suggest that managers can maximize the effectiveness of pre-briefing tools by pointing out when team members should share and integrate knowledge.

Contingency Planning: A Variation of Pre-briefing

Contingency planning helps teams and CSIRTs anticipate unexpected events by planning in advance how they might be handled. Thus, this strategy is particularly useful to help CSIRTs be more adaptive. Unexpected events will require a shift in the team's strategy. Contingency planning is intended to eliminate the chaos and confusion that can happen when unanticipated adverse events occur. The processes involved in contingency planning are similar to forecasting. For example, if a CSIRT comes up with a solution to mitigate a threat, that solution may have unintended consequences for which the team should forecast and determine plans for addressing. CSIRTs may also receive information about a new hacker or intrusion method and create a plan to prevent or end a possible future attack. Effective teams make use of their downtime or low workload periods by engaging in discussions around anticipated negative events and creating potential plans for dealing with them. Such discussions allow teams to be more proactive rather than reactive should those events occur.

Recommendations for Use:

To train CSIRT members in contingency planning, managers can use either past or anticipated events to describe attacks, threats, or unintended consequences of implementing particular solutions that have the highest probability of occurring. They can then encourage members to walk through a solution implementation plan and have them identify all of the information they have that is relevant to the plan being successful or not. Team members should also identify potential obstacles to a proposed action plan, and prepare possible responses. This kind of activity creates situational awareness and the ability to solve several problems as they arise (Bolstad et al., 2010).

Effectiveness Evidence:

Contingency planning has been demonstrated to increase situational awareness by 32% - 52% (Bolstad et al., 2010). It has also been shown to increase knowledge of how to deal with particular adverse events by 58% (Bolstad et al., 2010). These numbers suggest very positive effects for relatively simple additions to SBTs. Even if simulation training is not feasible, these tools can still be utilized with the instruction and guidance of a team leader for how to use them.

7.4.2 STRATEGY 2: USE A COUNTERFACTUAL THINKING APPROACH TO GET TEAM MEMBERS TO SHARE UNIQUE INFORMATION

Team members often do not realize that they have information that no one else knows. For this reason, they also fail to share it. Team members are more likely to discuss information that is held commonly among the members, a phenomenon called the shared information bias (Forsyth, 2009). That is, individuals are more likely to talk about information everyone knows as opposed to expertise or domain-specific knowledge that only one person might have (Baked, 2010). In order for collaborative problem-solving to be effective, team members must contribute their unique information to the group (see the problem-solving process model).

The goal of counterfactual thinking is to help team members become more aware of multiple solution options, and to devote more consideration to different decision options. This form of thinking can reduce premature decision closure in teams. Counterfactual thinking is a particular mindset that prompts team members to think about unique information they hold that otherwise they might not have shared; it is a relatively simple team discussion method that demonstrates high returns.

Recommendations for use:

Counterfactual thinking gets team members to think about what might have been (Galinsky & Kray, 2004). For example, teams would discuss what might have happened in a past situation or in a given scenario that is different from what actually happened. In a CSIRT context, this could involve members considering multiple possible consequences of particular previous incidents. They might explore what other possible outcomes could have occurred from the incident. Such discussions should result in members bringing different ideas and perspectives to the problem. For example, if a certain cyber exfiltration was limited to one private organization in a particular incident, managers prompting counterfactual thinking might explore with their team the different consequences that might have happened if this same exfiltration happened to a critical infrastructure organization or across several organizations within a critical infrastructure sector.

Counterfactual thinking helps team members explore different perspectives and contribute ideas and expertise that are not widely shared across the team. If managers and trainers want to demonstrate the existence of the tendency in teams not to share unique information, they can use exercises such as PB Technologies (Peterson, n.d.) or Tor Task Force (Greco & Thompson, n.d.). They can also use these exercises to practice other aspects of team problem solving. These exercises provide participants with different information about multiple candidates, and ask the team to determine which one is the most appropriate choice. Participants must combine their information to make the right choice. Training materials and instructor's guides for these exercises can be ordered from the following source: https://www.negotiationexercises.com

Effectiveness Evidence:

Teams using a counterfactual thinking prime (i.e., reminding participants to consider what might have happened differently) before discussing an incident shared 25% more unique information than teams who did not use the prime, and correctly solved the incident 66% of the time (compared to 23% for the non-prime teams; Galinksy, & Kray, 2004). The evidence suggests instilling a counterfactual mindset in CSIRT members with a 5-minute exercise can significantly improve their ability to engage in the problem-solving steps. By practicing this method during low-severity incidents, team members will remember to engage in different ways of thinking and consider more information during high-pressure situations as the process becomes habitual.

7.4.3 STRATEGY 3: PROVIDE TEAM FEEDBACK DURING STRUCTURED DEBRIEFING

Providing feedback to teams after resolving major incidents and when engaged in training simulations fosters more effective collaboration (Salas et al., 2008). Indeed, in simulation-based training, feedback has been shown to improve performance 26% more than for those who did not receive feedback (Domuracki, Wong, Olivieri, & Grierson, 2015). Many CSIRTs use debriefing (or lessons learned) after incident resolution, but these exercises are often too loosely structured to provide maximum benefits. Debriefing should entail walking the team through a particular incident and pointing out the breakdowns in teamwork that occurred at different phases of incident resolution. The training program, TeamSTEPPS, described in Chapter 5 ("Communication Effectiveness in Incidence Response") provides examples of several teamwork behaviors that can be examined in team feedback and debriefing sessions. Managers and trainers can retrieve information on this program at: www.teamstepps.ahrq.gov. While this program was developed specifically for healthcare professionals, facilitators can adapt its principles to CSIRTs.

When managers or facilitators give feedback, they often tend to focus mostly on team failures. However, in such sessions, they should also focus on teamwork successes. Managers need to share examples of what constitutes both effective and weak team performance (Ellis & Davidi, 2005). Indeed, teams who were given feedback on both their successes and failures demonstrated 83% better understanding of successful performance events one week later than those who did not receive similar feedback (Ellis & Davidi, 2005). Thus, when conducting debriefing sessions and providing feedback, managers and trainers should specifically ask for positive and negative instances of teamwork behaviors (e.g., communication) that occurred during the incident. Team members should pinpoint how those behaviors helped or hurt performance. If this debriefing process is to be used as part of a training simulation, the manager can videotape parts of the simulation and play them back for team members to see their teamwork behaviors in action.

Recommendations for Use:

Salas and colleagues (2008, pp. 520-521) specified 12 evidence-based principles for effective debriefing. These include the following behaviors:

1. Use debriefs as a tool to analyze team strengths and issues after specific incidents
2. Ensure that support for debriefs as a learning tool is communicated by higher management
3. Train team leaders and members to understand teamwork processes so that they can be recognized when assessing performance.
4. Ensure (through training) that team leads know the fundamentals of conducting team debriefs.
5. Encourage team members to feel comfortable sharing constructive criticism during debriefs.
6. Limit the number of topics for each debriefing.
7. Provide feedback on specific teamwork interactions that occurred during the performance episode from which the debrief is based.
8. Provide specific examples when providing performance feedback.
9. Concentrate more on feedback related to teamwork processes and less on overall final outcomes.
10. Give individual and team feedback, but know in what setting each should be given.
11. Provide performance feedback as soon as possible.
12. Document conclusions and goals set during the debrief.

Please see Salas, et al. (2008) for additional information. This material can be acquired through the following website: http://www.ingentaconnect.com/content/jcaho/jcjqs/2008/00000034/00000009/art00003. A debriefing assessment tool can also be found at this website: https://www.ahn.org/sites/default/files/file/D11DASH-handbook2010FinalRev2.pdf. While developed for medical teams, it can be easily adapted to CSIRTs.

Effectiveness Evidence:

Like pre-briefs, debriefs also create a shared awareness of the collective teams' behaviors that constitute effective teamwork. Research has shown that teamwork mental models (i.e., shared ideas of effective teamwork) were 29% more accurate for teams who underwent structured debriefing than for those who did not engage in such feedback sessions (Smith-Jentsch, Cannon-Bowers, Tannenbaum & Salas, 2008). Teams who were pre-briefed and debriefed engaged in 33% more supportive behaviors and 41% more information exchange. They were also 111% as likely to have a better shared understanding of the situation than teams who did not engage in debriefing (Smith-Jentsch et al., 2008). Teamwork dimensions, such as "[maintaining] team structure and climate, [applying] problem solving strategies, [supporting] the team with information, [executing] plans and [managing] workload, and [improving] team skills," increased an average of 23% after structured feedback and debriefing (Shapiro et al., 2004, p. 420).

Research using a hospital emergency room simulation shows that the combination of both pre-briefing and debriefing provides strong gains for teamwork (Weld, et al., 2015). This simulation included a relatively short preoperative briefing that used a checklist to ensure all key information was covered in the session. After the surgery, a debriefing was held for 5 minutes with just surgery team members to identify any patient safety issues (Weld et al., 2015). After employment of pre-briefing and debriefing, safety issues were reduced from 16% to 6% (Weld et al., 2015). Specifically, the average time to complete a surgical case was 12.7 minutes less after teamwork training and post-operative briefings (Weld et al., 2015). Further, the number of surgeries that began on time increased by 21% (Weld et al., 2015). The results indicated by this simulation suggest that structuring the problem-solving process and the lessons-learned afterwards through pre-briefs and debriefs are important processes that should be adopted by CSIRTs.

7.4.4 STRATEGY 4: DEVELOP ADAPTIVE THINKING BY PROVIDING EXPLORATORY OR ACTIVE LEARNING EXPERIENCES WITH WIDE PROBLEM VARIETY

Managers can use forms of *exploratory or active learning* to develop adaptive thinking skills. This approach can be used in a formal training simulation as a series of developmental work experiences, and even as a form of self-development. Active learning involves individuals exploring and solving a new problem with little or no formal instruction (Bell & Kozlowski, 2008). These learners determine on their own how they would approach a problem, what knowledge they need to solve the problem, where they need to acquire such knowledge, what should be the nature of the best solutions, and how they would derive such solutions. For example, a CSIRT manager can provide the team with exercises in which they need to solve novel incidents or system intrusions. The exercises provided to learners should have significant variety, where they have to use very different kinds of solutions to solve different problems.

Recommendations for Use:

To use this approach, managers should provide novel learning opportunities to their team. Team members are urged to work on these problems on their own or as a team. Managers can provide information to members on how they can learn new strategies related to the problem. They should also encourage them to change how they are thinking about a particular problem by using such frame-changing prompts as:

- How is this problem different from the other problems you faced?
- What is a different way of thinking about this problem?
- What other possible solutions might apply to this problem?
- How will the solution to this problem need to be different from other previous solutions?
- Are we thinking about this incident in the right way?
- What happens if this solution is wrong?
- How might a hacker or adversary respond to this solution?

Managers should provide CSIRT members with multiple kinds of problems that require very different kinds of solutions. These active learning experiences can be provided as part of a formal training or gaming exercise, or as a series of developmental assignments provided to CSIRT members as part of their work duties. Managers can also encourage their team members to find and pursue different cybersecurity challenges as part of their personal self-development.

Effectiveness Evidence:

Several studies have shown that different forms of active and exploratory learning strategies produced higher adaptive performance (Bell and Kozlowski, 2008; Keith & Frese, 2008). For example, in one study, trainees who engaged in exploratory learning showed higher adaptive performance (11%) than trainees who did not; trainees who received prompts to treat errors while engaging in exploratory learning also showed higher adaptive performance (31%) than those who did not engage in exploratory learning (Keith & Frese, 2005). In another study, individuals who practiced a variety of different problems achieved higher adaptive performance (10%) compared to those who practiced a series of similar types of problems (Holladay & Quiñones, 2003). In a third study, the trainees who experienced problem variety in practice trials along with frame-changing prompts had higher adaptive decision making performance (37%) compared to a control group (DiRosa, Nelson, Gulick, Conjar, & Zaccaro, 2009). Other studies have also shown that having a variety of developmental work assignments (Horn, 2009) and self-development experiences (Langkamer, 2009) were also associated with stronger adaptation.

These studies support the recommendation that managers can improve adaptation skills in their team by providing members with a wide variety of learning activities in which they explore solutions on their own or with others on their team. Managers should support such learning by (a) encouraging their subordinates to treat errors in these activities as learning opportunities and (b) prompting them to consider different perspectives when approaching learning problems (see Chapter 11, “Continuous Learning in Incident Response,” for more information on this training approach).

CONSIDERATIONS FOR MULTITEAM SYSTEMS

7.4.5 STRATEGY 5: TRAIN LEADERS TO PRE-PLAN STRATEGIES FOR HOW MULTIPLE TEAMS WILL WORK TOGETHER

Multiteam problem-solving can also be improved using the pre-planning strategies discussed earlier. As explained in Chapter 5 (“Communication Effectiveness in Incident Response”; see leader boundary spanning), between team communication is often more efficient when one person is designated as the point of contact. A similar principle applies here. Team leaders in an MTS can work together to engage in pre-planning that maps out (a) how multiple teams will work together, and (b) how each of those teams will coordinate their actions with other specific teams. Creating a strategy for MTS problem solving (or mapping out how multiple teams need to work together) involves:

- Acquiring information about how closely teams need to work together to solve the problem (i.e. how interrelated their actions are);
- Organizing information about how each team will contribute to the mission; and
- Communicating this information to each component team before the mission begins so that everyone has a shared understanding of how they will work with other teams.

Recommendations for Use:

Leaders can be trained to engage in pre-planning for MTSs using simulation exercises that require multiple teams to work closely together. Managers or facilitators should describe effective planning processes at the MTS level and then demonstrate how to develop those plans. One example of such a training program provided leaders with four situations where they could anticipate and determine how each team’s actions should be timed and ordered to solve a designated problem effectively (DeChurch & Marks, 2006). In this kind of training, trainees practice different scenarios where they actually map out component teams' actions, communicate their plan to each component team, and receive structured feedback on the plan they created to address the problem and how they communicated it (DeChurch & Marks, 2006).

To be effective, this training should also inform leaders of how to monitor the interaction (or joint activities) of component teams by (a) assessing their locations and progress, and (b) communicating this information to other teams (DeChurch & Marks, 2006). For example, leaders can observe multiple teams working, assess their progress levels, and report that progress to other teams involved. To help leaders understand proper assessment and communication behaviors, leaders can be shown videos that simulate proper or improper leader behaviors and have each positive or negative behavior pointed out and explained (DeChurch & Marks, 2006). Leaders in the training can then be asked to point out instances themselves where one team's progress should be communicated to other teams working jointly on a problem. They can then be given feedback based on how well they identified the correct instances (DeChurch & Marks, 2006).

Effectiveness Evidence:

Pre-planning strategies for MTS collaboration have been shown to improve MTS leadership behaviors. Training for mapping out a between-team strategy and coordinating between-team actions have improved MTS leadership by 68% (DeChurch & Marks, 2006). Training in only coordination still results in a 68% increase in MTS leadership, while training only in mapping out between-team problem solving strategy results in a 54% improvement in MTS leadership. Leader training is important for improving inter-team coordination, which leads to effective MTS collaboration and performance in problem solving situations (DeChurch & Marks, 2006).

CONSIDERATIONS FOR TEAM STAFFING

7.4.6 STRATEGY 6: STAFF YOUR CSIRT WITH TEAM MEMBERS WHO HAVE A TEAM ORIENTATION AND TEAMWORK SKILLS

A well thought out staffing plan can increase the effectiveness of team collaboration and collective problem-solving. Having the right mix of people on a team determines the quality of work that team can produce (Mathieu, Tannenbaum, Donsbach, & Alliger, 2014). Specifically, high levels of team skills such as cooperativeness, team orientation, and organizing skills, shared by all team members, will enable the team to build the levels of trust and SKUE that, in turn, foster effective collaborative problem-solving (Mathieu et al., 2014). Teamwork skills such as cooperativeness and team orientation have consistently demonstrated medium to large positive effects on team performance (Bell, 2007), translating to a performance improvement of 10-25%.

Recommendations for Use:

Follow the seven-step process described below, derived from Mathieu et al., (2014), in order to properly staff a CSIRT and engage in effective collaborative problem-solving.

7.5 Chapter Summary

The nature of CSIRT work is knowledge work that typically involves multiple team members working together to solve complex problems (as described in table 7.1). CSIRTs must be able to engage in the processes of situational awareness, collective information processing and forecasting in order to be effective in solving novel problems. Managers can improve these processes using strategies such as pre-briefing, debriefing, simulations, and focused feedback-giving. Leaders and managers themselves can develop the leadership skills that will help them facilitate collaborative problem-solving in their teams (such as MTS pre-planning and contingency planning). In the next two chapters, Chapters 8 ("Shared Knowledge of Unique Expertise") and 9 ("Trust in Teams and Incident Response Multiteam Systems"), we describe two team states that are important for successful collaboration as well as strategies to create or improve them in CSIRTs. Managers should consider these recommendations in conjunction with those described in this chapter to maximize CSIRT functioning.

TABLE 7.4 CSIRT STAFFING

STEP	CONSIDERATIONS AND IMPLEMENTATION SUGGESTIONS
1. Describe the Team	*Ask yourself:* • What are the positions on the team? • Are any positions particularly critical for success? • How much do team members need to interact in order for the team to be successful? • Who are the existing team members? *Tips:* • Determine which positions will be changed as you are working on staffing your CSIRT. If you find that a position is particularly critical (e.g., a team leader or a member who frequently works with other teams in the CSIRT), spend more time and resources ensuring that position is adequately staffed. • If you think the task work of your CSIRT requires extensive interaction between team members, teamwork competencies will likely be very important.

TABLE 7.4 CSIRT STAFFING (CONTINUED)

STEP	CONSIDERATIONS AND IMPLEMENTATION SUGGESTIONS
2. Clarify Requirements	*Ask yourself:* • What are the specific requirements for the position on your CSIRT? • Are there any MTS or organization-level considerations you need to account for when staffing your CSIRT? These could include an interest in increasing diversity or staffing the CSIRT with members who have a particular type of experience. *Tips:* • Consider both the task work and teamwork requirements when staffing your CSIRT. Identify the knowledge, skills, and abilities (KSAs) that the work requires and rank order them, as tradeoffs may be necessary. If ranking is difficult, rate KSAs as "must have" or "nice to have" for the role. • Think about the KSAs that your team members already have in place. Do you need to staff your CSIRT with members who have the same types of KSAs, or do you need complementary skills? For example, if your team already has 2 or 3 members who are skilled in forensics, you may want to consider a member who has a different background to round out the experience of your CSIRT. • Consider the goals and mission of your organization. Some organizational-level considerations may be required to create a developmental assignment for a rising manager or to fulfill the organization's diversity mission.
3. Establish the Candidate Pool	*Ask yourself:* • Who is eligible, available, and interested in joining the team? • What are the needs of the component team in relation to the entire CSIRT MTS and the organization as a whole? *Tips:* • Consider your knowledge of the interpersonal dynamics between members of your CSIRT. Are there members who work particularly well together? Conversely, are there members who are likely to clash? • There may be a strong candidate for one of your component teams within your CSIRT but this person may already be earmarked for a leadership position elsewhere in the CSIRT. Ensure that you are thinking within the broader organizational context as you are staffing your CSIRT MTS.
4. Assess Candidates	*Ask yourself:* • What are the individual task work skills of the candidates? • What are the individual teamwork skills of the candidates? • How well do you think the candidates would fit with existing members of the CSIRT? *Tips:* • Assess the candidate's overall fit to the position, and to the dynamics of your CSIRT, considering the broader context of the MTS and organization. • Compare the candidate's KSAs to those of the existing CSIRT members. Check for overlaps and gaps to ensure that you are staffing the team with a new member who will complement the existing structure.
5. Tentatively Assign Candidates	*Ask yourself:* • What is the logical way to assign a candidate to each open position? *Tips:* • Considering all of the factors at the team, CSIRT MTS, and organizational level you are aware of, tentatively assign candidates to open positions. • Iterate steps 5 – 7 in order to make adjustments until you are satisfied with the team's composition.
6. Assess the Proposed Team Composition	*Ask yourself:* • Is each position now filled with an individual who has the requisite skills or at least can quickly learn them? • Do the most important positions, as identified in step 1, have high quality candidates assigned to them? • Does the proposed composition plan meet the component team, CSIRT MTS, and organization requirements? • How well do you anticipate the proposed candidates will work together? *Tips:* • You may find yourself faced with tradeoffs. For example, in order to get a high quality candidate into an important position, you may need to sacrifice another position on the team.
7. Adjust the Proposed Membership and/or Plan Compensatory Actions	*Ask yourself:* • Do you need to adjust the proposed plan before finalizing it? • Are there any compensatory actions you want to plan to help your team staffing plan succeed (e.g., coaching, training, or other forms of support)? *Tips:* • If you decide to adjust your staffing plan, examine each potential solution and rank the solutions in order of how well they meet the requirements laid out in step 2. • Consider the actions that might help the new team member(s) assimilate into the team and build trust. These may include onboarding, training sessions, or informal conversations with experienced CSIRT members to help the new member(s) get off to a fast start.

References

Adis, C.S. (2013). *The role of cognitive capacity and information process preferences in forecasting and prediction accuracy*. (Doctoral dissertation). Retrieved from http://search.proquest.com.mutex.gmu.edu/pqdtlocal1006610/index

Alison, L., van den Heuvel, C., Waring, S., Power, N., Long, A., O'Hara, T., & Czrego, J. (2013). Immersive simulated learning environments for researching critical incidents: A knowledge synthesis of the literature and experiences of studying high-risk strategic decision making. *Journal of Cognitive Engineering and Decision Making, 7*, 255-272.

Baard, S.K., Rench, T.A., Kozlowski, S.W.J. (2014). Performance adaptation: A theoretical integration and review. *Journal of Management, 40*, 48-99.

Baked, D. F. (2010). Enhancing group decision making: An exercise to reduce shared information bias. *Journal of Management Education, 34*, 249-279.

Bell, S. T. (2007). Deep-level composition variables as predictors of team performance: a meta-analysis. *Journal of Applied Psychology, 92*, 595-615.

Bell, B. S., & Kozlowski, S. W. J. (2009). Toward a theory of learner-centered training design: An integrative framework of active learning. In S. W. J. Kozlowski & E. Salas (Eds.), *Learning, training, and development in organizations* (pp. 263-300). New York: Routledge.

Bolstad, C. A., Endsley, M. R., Costello, A. M., & Howell, C. D. (2010). Evaluation of computer-based situation awareness training for general aviation pilots. *The International Journal of Aviation Psychology, 20*, 269-294.

Byrne, C. L., Shipman, A. S., & Mumford, M. D. (2010). The effects of forecasting on creative problem-solving: An experimental study. *Creativity Research Journal, 22*, 119-138.

Clark, A., & Chalmers, D. (1998) . The extended mind. *Analysis, 58*, 7-19.

DeChurch, L. A., & Marks, M. A. (2006). Leadership in multiteam systems. *Journal of Applied Psychology, 91*, 311-329.

DeYoung, C. G., Flanders, J. L., & Peterson, J. B. (2008). Cognitive abilities involved in insight problem solving: An individual differences model. *Creativity Research Journal, 20*, 278-290.

DiRosa, G., Nelson, J., Gulick, L., Conjar, E. A., & Zaccaro (2009). *The effects of experiential variety and metacognition on adaptive performance*. Poster presented at the 24th annual meeting of the Society for Industrial and Organizational Psychology, New Orleans, LA, April 2009.

Domuracki, K., Wong, A., Olivieri, L., & Grierson, L. E. (2015). The impacts of observing flawed and flawless demonstrations on clinical skill learning. *Medical education, 49*, 186-192.

Edmondson, A.C., & Lei, Z. (2014). Psychological safety: The history, renaissance, and future of an interpersonal construct. *Annual Review of Organizational Psychology and Organizational Behavior, 1*, 23-43.

Ellis, A. P., Bell, B. S., Ployhart, R. E., Hollenbeck, J. R., & Ilgen, D. R. (2005). An evaluation of generic teamwork skills training with action teams: effects on cognitive and skill-based outcomes. *Personnel psychology, 58*, 641-672.

Ellis, S., & Davidi, I. (2005). After-event reviews: drawing lessons from successful and failed experience. *Journal of Applied Psychology, 90*, 857-871.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors: *The Journal of the Human Factors and Ergonomics Society, 37*, 32-64.

Fiore , S. M., Smith-Jentsch, K. A., Salas, E., Warner, N., & Letsky, M. (2010). Towards an understanding of macrocognition in teams: developing and defining complex collaborative processes and products. *Theoretical Issues in Ergonomics Science, 11*, 250-271.

Forsyth, D. R. (2009). *Group dynamics (5th ed.)*. Pacific Grove, CA: Brooks/Cole.

Galinsky, A. D., & Kray, L. J. (2004). From thinking about what might have been to sharing what we know: The effects of counterfactual mind-sets on information sharing in groups. *Journal of Experimental Social Psychology, 40*, 606–618.

Greco, M., & Thompson, L. (n.d.). Tor Task Force. Retrieved from https://www.negotiationexercises.com/Details.aspx?ItemID=343

Holladay, C. L., & Quiñones, M. A. (2005). Reactions to diversity training: An international comparison. *Human Resource Development Quarterly, 16*, 529-545.

Hong, Y. Y., Morris, M., Chiu, C. Y., & Benet-Martínez, V. (2000). Multicultural minds: A dynamic constructivist approach to culture and cognition. *American Psychologist, 55*, 709-720.

Horn, Z.N.J. (2008). Examining the influence of stretch assignments on adaptive outcomes: The importance of developing complex frames of reference. (Doctoral dissertation). Retrieved from http://search.proquest.com.mutex.gmu.edu/pqdtlocal1006610/index

Keith, N., & Frese, M. (2005). Self-regulation in error management training: Emotion control and metacognition as mediators of performance effects. *Journal of Applied Psychology, 90*, 677– 691.

Keith, N., & Frese, M. (2008). Performance effects of error management training: a meta-analysis. *Journal of Applied Psychology, 93*, 59-69.

Koles, K.L.K. (2001)/ *The impact of feedback-induced self-attention on antecedents of team performance*. (Doctoral dissertation). Retrieved from http://search.proquest.com.mutex.gmu.edu/pqdtlocal1006610/index

Langkamer, K.L. (2008). *Development of a nomological net surrounding leader self-development*. (Doctoral dissertation). Retrieved from http://search.proquest.com.mutex.gmu.edu/pqdtlocal1006610/index

Mathieu, J. E., Tannenbaum, S. I., Donsbach, J. S., & Alliger, G. M. (2014). A review and integration of team composition models moving toward a dynamic and temporal framework. *Journal of Management, 40*, 130-160.

Miller, D., Price, J. M., Entin, E., Rubineau, B., & Elliott, L. (2001, October). Does planning using groupware foster coordinated team performance? *In Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 45, No. 4, pp. 390-394). SAGE Publications.

Mumford, M.D., Lonergan, D.C., & Scott, G. M. (2002). Evaluating creative ideas: Processes, standards, and context. *Critical Inquiry, 22*, 21-30.

Mumford, M. D., Mecca, J. T. & Watts, L. I. (2015). Planning processes: Relevant cognitive operations. In M. D. Mumford & M. Frese (Eds.), The psychology of planning in organizations: Research and applications. New York: Routledge.

Mumford, M. D., Medeiros, K. E. and Partlow, P. J. (2012), Creative thinking: Processes, strategies, and knowledge. *The Journal of Creative*

Behavior, 46, 30–47.

Mumford, M. D., Mobley, M. I., Reiter-Palmon, R., Uhlman, C. E., & Doares, L. M. (1991). Process analytic models of creative capacities. *Creativity Research Journal, 4*, 91-122.

Nelson, J. K., Zaccaro, S. J., & Herman, J. L. (2010). Strategic information provision and experiential variety as tools for developing adaptive leadership skills. *Consulting Psychology Journal: Practice and Research, 62(2)*, 131-142.

Orasanu, J. (1994). Shared problem models and flight crew performance. In N. Johnston, N. McDonald, & R. Fuller (Eds.), *Aviation psychology in practice* (pp. 255–285). Brookfield, VT: Ashgate.

Oser, R.L., Gualtieri, J.W., Cannon-Bowers, J.A. & Salas, E. (1999). Training team problem-solving skills: an event-based approach. *Computers in Human Behavior, 15*, 441-462.

Peterson, R. (n.d.). PB Technologies. Retrieved from https://www.negotiationexercises.com/Details.aspx?ItemID=143

Pulakos, E. D., Arad, S., Donovan, M. A., & Plamondon, K. E. (2000). Adaptability in the workplace: Development of a taxonomy of adaptive performance. *Journal of Applied Psychology, 85*, 612–624.

Rentsch, J.R., Delise, L.A., Mello, A.L. & Staniewicz, M.J. (2014). The integrative team knowledge building training strategy in distributed problem-solving teams. *Small Group Research, 45(5)*, 568-591.

Rouse, W. B., & Morris, N. M. (1986). On looking into the black box: Prospects and limits in the search for mental models. *Psychological bulletin, 100*, 349-363.

Salas E, Klein C, King H, Salisbury M, Augenstein JS, Birnbach DJ, Robinson DW, Upshaw C. (2008).Debriefing medical teams: 12 evidence-based best practices and tips. Jt Comm J Qual Patient Saf 2008;34:518–27.

Shapiro, J. J., Morey, J. C., Small, S. D., Langford, V., Kaylor, C. J., Jagminas, L., et al. (2004). Simulation based teamwork training for emergency department staff: Does it improve clinical team performance when added to an existing didactic teamwork curriculum? *Quality and Safety in Health Care, 13*, 417–421.

Smith-Jentsch, K. A., Cannon-Bowers, J. A., Tannenbaum, S. I., & Salas, E. (2008). Guided team self-correction impacts on team mental models, processes, and effectiveness. *Small Group Research, 39*, 303-327.

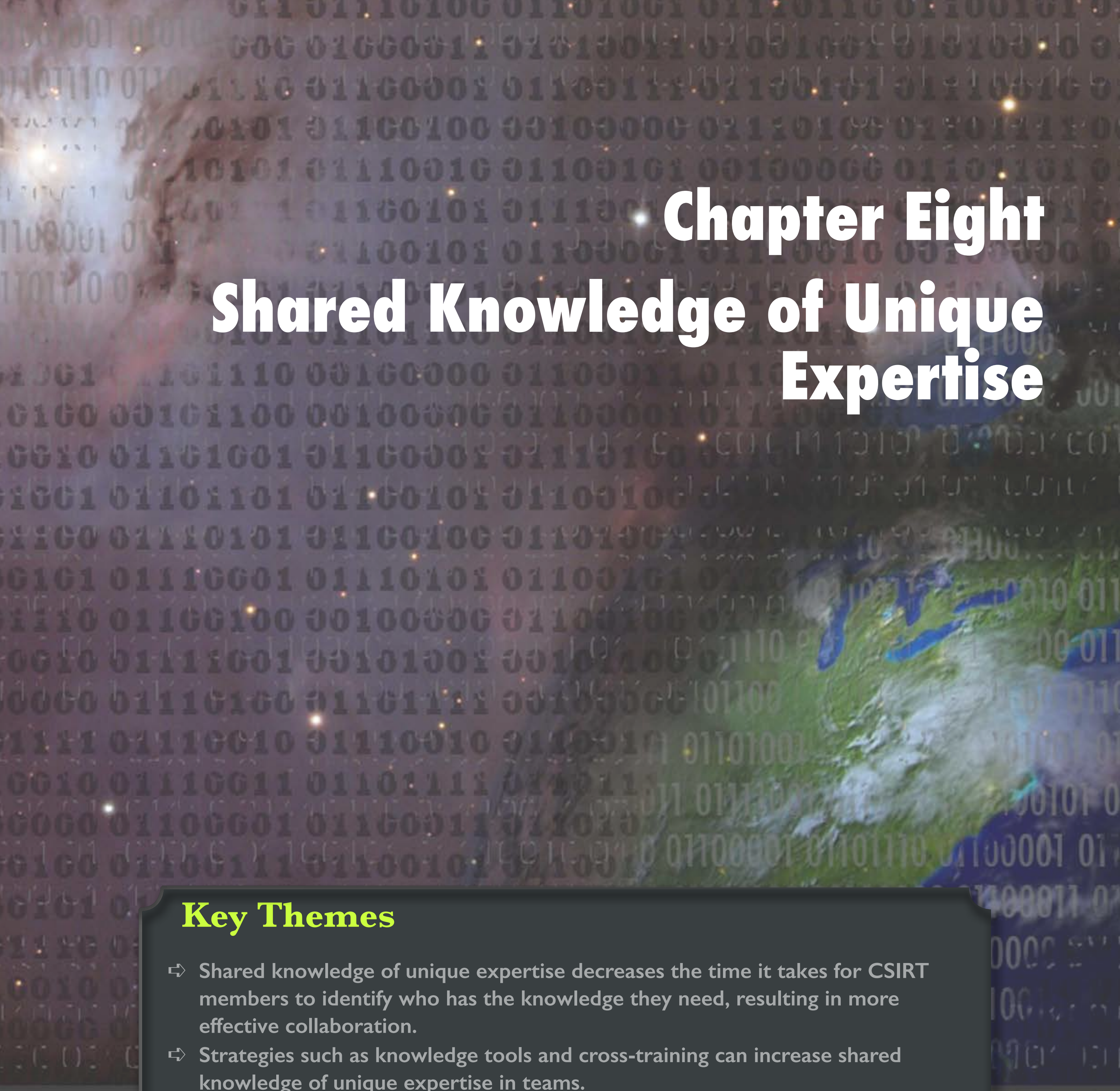
Sparks, J. (2015, June) Effective team leadership and process improvement for network security operations. Paper presented at the 27th Annual FIRST Conference, Berlin, Germany.

Stout, R. J., Cannon-Bowers, J. A., Salas, E., & Milanovich, D. M. (1999). Planning, shared mental models, and coordinated performance: An empirical link is established. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 41*, 61-71.

Weld, L.R., Stringer, M,T., Ebertowski, J.S., Baumgartner, T.S., Kasprenski, M.C., Kelley, J.C., Cho, D.S., Tieva, E.A. & Novak, T.E. (2015). TeamSTEPPS improves operating room efficiency and patient safety. *American Journal of Medical Quality, 1062860615583671*, 1-7.

Zaccaro, S. J., Hargrove, A. K., Chen, T. R., Repchick, K. M., & McCausland, T. C. (2016). A comprehensive multilevel taxonomy of cybersecurity incident response performance. In S. J. Zaccaro, R. S. Dalal., L. E. Tetrick, and J. A. Steinke (Eds.), *Psychosocial Dynamics of Cyber Security (13-55)*. New York: Routledge.

Zyphur, M. J. (2009). When mindsets collide: Switching analytical mindsets to advance organization science. *Academy of Management Review, 34*, 677–688.



Chapter Eight

Shared Knowledge of Unique Expertise

Key Themes

- Shared knowledge of unique expertise decreases the time it takes for CSIRT members to identify who has the knowledge they need, resulting in more effective collaboration.
- Strategies such as knowledge tools and cross-training can increase shared knowledge of unique expertise in teams.

Contents

8.0 Introduction

In Chapter 7, “Collaborative Problem-Solving in Incident Response,” we described the steps necessary for effective collaborative problem-solving in CSIRTs. We also noted two team attributes, team knowledge and team trust, that enhance CSIRTs’ abilities to engage in these steps quickly and effectively. This chapter describes one form of team knowledge, while the next chapter covers team trust.

The first step in the CSIRT problem-solving process is identifying that an attack or threat is actually present and understanding its parameters. One team attribute that significantly enhances each member’s ability to identify and classify problems is *shared knowledge of unique expertise* (SKUE). SKUE refers to the knowledge team members have of each other team member's particular expertise and experiences. Called "transactive memory" by some (Wegner, 1986; Austin, 2003), this notion reflects the idea that team members in a CSIRT likely have different areas of expertise that can be useful when solving different kinds of cybersecurity events and incidents. However, all members need to have the same knowledge of “*who knows what*.” Likewise, when working in CSIRT multiteam systems (MTSs; see Chapter 2, “The Social Maturity of CSIRTs and Multiteam Systems”), members of different teams need to share knowledge of the functional roles of other teams and also what expertise individuals in those teams possess. Such knowledge creates a shared awareness in the team or MTS that is crucial for problem-solving.

8.1 Assessing Shared Knowledge of Unique Expertise

The following assessment exercise is designed to provide managers with a diagnostic tool in order to determine how well the CSIRT, individuals, or component teams within the CSIRT MTS possess SKUE. This will ultimately help determine the social maturity of the CSIRT (See Chapter 2, “The Social Maturity of CSIRTs and Multiteam Systems,” for additional information). Based on the responses to this assessment, managers can determine whether they would benefit from the strategies offered in this chapter. Managers should consider the time and resources required to implement these strategies relative to their need for improvement.

Assess how your CSIRT is functioning in this area by responding to the following assessment on a 1-5 scale where 1= Strongly Disagree, 2= Disagree, 3= Neither Agree nor Disagree, 4= Agree, 5= Strongly Agree.

> “We have specializations. Nobody can be good at everything … everybody uses others’ knowledge.”
>
> ~ CSIRT Member

GO TO PAGE 141 FOR
STRATEGIES FOR CSIRT MANAGER

8.2 Background

CSIRTs confront many different types of events, and several incidents are often new to the analysts tasked with resolving them. Thus, a less experienced analyst might tag an incident that looks suspicious but not have the experience or knowledge to classify it or determine how to resolve it. However, more experienced team members have likely resolved similar types of incidents in the past. If the first analyst knows of the other team

> “…we know a lot about everyone’s skill set because we work so closely together on a day to day basis. I think everyone has a few people they know who to go to for certain types of questions.”
>
> ~ CSIRT Member

ASSESSMENT EXERCISE

1. My team members know exactly who has the knowledge to handle a particular incident.
2. My team members can explain “who knows what” within the team.
3. Members of my team ask the right person for information.
4. In team meetings, members appear to know what other people within the team know.
5. Members of my team communicate what knowledge they possess to other team members.
6. My team members know exactly which team in our CSIRT MTS has the right knowledge/expertise to handle a particular incident.
7. My teams explain “which teams know what” within the CSIRT MTS.
8. Members of my team ask the right team in a CSIRT MTS for information.
9. Members of my team communicate what knowledge they possess to other teams in the CSIRT MTS.

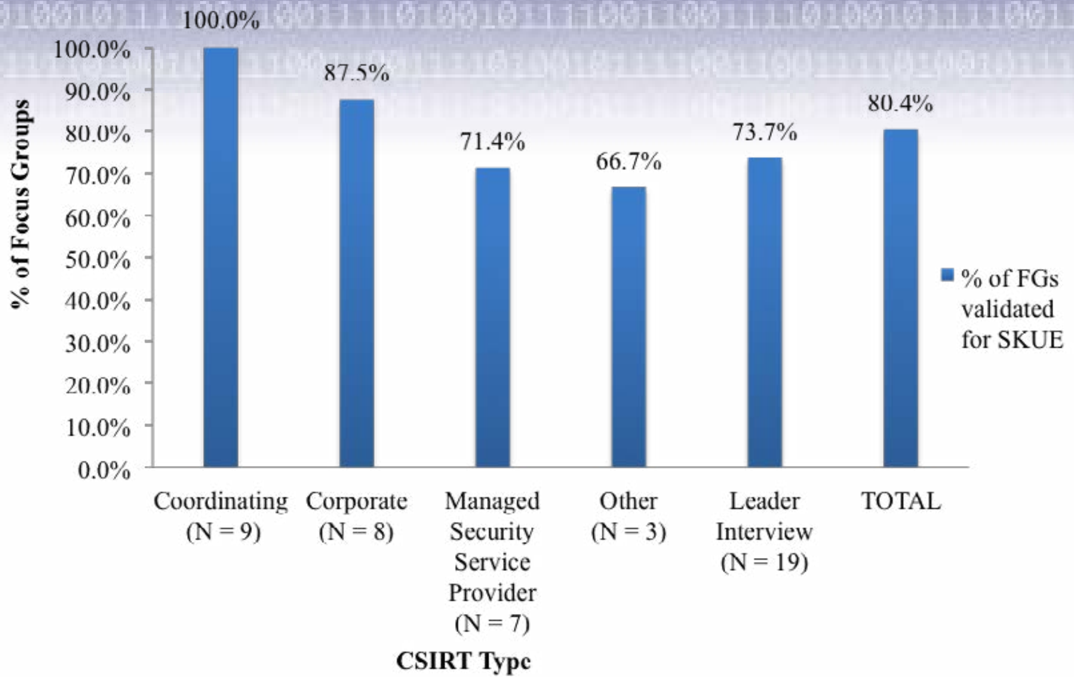


Figure 8.1 Focus Group Support for SKUE

members' experiences and expertise, that analyst can call on the right person for advice or collaborate with that person to resolve the incident more quickly.

Knowing the unique experiences and expertise each team member possesses also helps those who receive incident reports assign them to the right persons for triage and analysis. For example, when a member of a CSIRT forensics team has an unusual incident to investigate that requires collaboration and coordination with other stakeholders, knowing which team member (or which team in the CSIRT MTS) has the necessary social or professional networks in place with those stakeholders will increase the chances of quick resolution. Such collaboration can help CSIRTs reduce incident response time and provide accurate solutions to incidents. Providing information about past experiences and skills also fosters the formation of trust within and between teams (See Chapter 9, "Trust in Teams and Incident Response Multiteam Systems"). Thus, SKUE---knowing who knows what—is a very important driver of CSIRT performance.

> **"So if I have expertise in cryptography, for example, they'll send me in that role, if I'm available, of course. But if it's more about infrastructure, maybe they will find someone else ...We have specialists all over the place."**
>
> **~ CSIRT Member**

8.3 Project Findings

In 80% (37 out of 46) of the focus groups we conducted, CSIRT members and managers indicated that knowing who had what expertise on the team was among the most important team and MTS attributes for CSIRT effectiveness. These focus group participants noted that such knowledge helped incident responders identify the nature of unusual events, triage them faster, and develop effective solutions. Our interviews indicated that successful teamwork (within and between teams) in response to an incident began with the identification of people who had the most appropriate expertise to work on that particular incident. Figure 8.1 summarizes data from our focus groups indicating how often SKUE was mentioned as important in different types of CSIRTs and MTSs.

We also found confirmation of the importance of SKUE for cybersecurity incident response through a survey distributed to approximately 90 cybersecurity professionals. The survey asked these professionals to rate 46 knowledge, skills, abilities, and other attributes (KSAOs) on their importance for performing well as a cybersecurity incident response analyst. In that survey, "knowing what other team members know" was rated as important by 73 of 87 (84%) individuals.

8.4 Developing Shared Knowledge of Unique Expertise

In the following section, we provide exercises and recommendations for developing or increasing SKUE. These exercises and recommendations are based on the background information

> **Interviewer: How do you get to know what everyone knows?**
> **CSIRT Member: We have it written down on paper explicitly.**

and findings by our project team described in the previous section. Please use the assessment exercise at the beginning of this chapter to evaluate the effectiveness of SKUE in your CSIRT, and to help you determine the best strategies to improve your team.

8.4.1 STRATEGY 1: ESTABLISH KNOWLEDGE TOOLS (E.G. INFORMATION BOARD, KNOWLEDGE MAP) THAT DISPLAY MEMBERS' EXPERTISE, KNOWLEDGE, SKILLS, AND EXPERIENCES

Effective problem-solving in teams is dependent upon the creation and sharing of knowledge around particular incidents (Nemeth, O'Conner, Klock, & Cook, 2006). Knowledge tools are visual representations of team expertise designed to facilitate the creation and sharing of knowledge in teams (Chapter 7, "Collaborative Problem-Solving in Incident Response"; Rentsch, et al., 2010). Knowledge tools can include *information boards* (either virtual, to accommodate virtual team members, or physical), and *knowledge maps* or *knowledge banks*.

An information board allows all members with access to see information posted by other team members that is either incident-related or expertise-related. Information boards can also be used to track different phases of incident resolution. Such information boards can also be established or adapted to include the expertise and unique functions of different teams within a CSIRT MTS. These boards would map out the particular knowledge possessed by the different component teams, and the purposes of these teams in different phases of incident response. The completed information board is then distributed to all team leads in the CSIRT MTS.

In knowledge maps and banks, each team member's expertise is gathered, mapped out, and distributed to the entire team, so that all team members are aware of what they know as a team and what each team member knows individually. For example, expertise could include information about team members' familiarity with certain tools (e.g., applications, programming languages). Knowledge maps help team members to identify important knowledge in teams and navigate where to find certain knowledge among people, documents or databases (Davenport & Prusak, 1998). See Figure 8.2 for a sample knowledge map that

> **We made explicit whose responsibility it is to maintain an active view on certain subjects. So we know that this person is expected to know about this or expected to know about that, so whenever something comes up we know to whom to turn. And because we have these active discussions on who will be the person in charge of this or that subject, so in that sense we do know very accurately who we can contact.**
>
> **~ CSIRT Member**

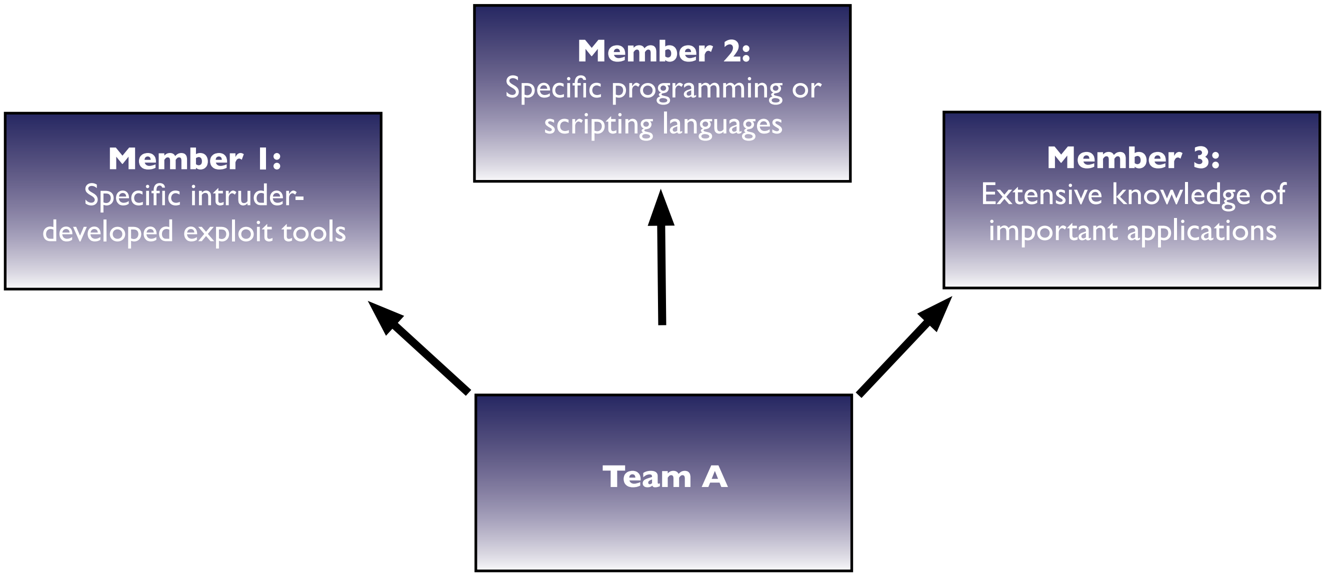

Member 2:
Specific programming or scripting languages
Member 1:
Specific intruder-developed exploit tools
Member 3:
Extensive knowledge of important applications
Team A

Figure 8.2 Example of a Team Knowledge Map Depicting Members of a Team and Their Areas of Expertise (or Specialist Skills)

indicates the distribution of member expertise about different client types. Lastly, team members will feel comfortable sharing their expertise, experiences, or lack thereof, in a trusting environment (See Chapter 9, "Trust in Teams and Incident Response Multiteam Systems").

Aside from individual knowledge and expertise, MTSs can also use knowledge maps to document each team's area of expertise/function. This can be broken out further if members within teams have their own areas of focus. Below, we provide recommendations for using knowledge tools in teams and MTSs.

Recommendations for Use:

We recommend the following when implementing a knowledge tool:

- Collect information about team members' educational and professional training background. Such information could include, but is not limited to, areas of specialization acquired, expertise and familiarity with certain software programs, programming languages, prior experiences with different types of stakeholders, and prior experience with specific malware (e.g., worms, viruses).
- Ask team members to indicate both the areas where they have expertise and those where they require more knowledge.
- Share collected knowledge and knowledge gaps with all team members.
- Evaluate the distribution of knowledge within a team and coordinate the assignment of specific knowledge subjects to team members.
- Encourage team members to make use of existing knowledge tools when needing information.
- In a CSIRT MTS, collect similar information about the different component teams. Evaluate the distribution of knowledge across the MTS, and coordinate assignment of specific knowledge areas to particular teams.

To maximize effectiveness, we recommend that these guides be:

- Developed at earlier rather than later stages in building a team
- Updated on a regular basis, or, at least, whenever members join the CSIRT, leave the CSIRT, or acquire new knowledge and expertise (e.g. complete additional training).

Effectiveness Evidence:

Research has demonstrated the effectiveness of information boards, both virtual and physical, and knowledge maps for increasing SKUE and improving subsequent collaborative problem-solving. Teams trained in the use of such boards had 12% more knowledge of other team members' roles than teams who were not trained (Rentsch et al., 2010); teams that used knowledge maps to acquire background information about team members had 36% more accuracy of SKUE, and team member agreement about the skills each member possessed increased by 138% (Schreiber & Engelmann, 2010).

> **"Everybody in the team is responsible for one topic to kind of research and does an article, and then does a presentation to the rest of the group."**
>
> **~ CSIRT Member**

The use of information boards during team training exercises resulted in members sharing 68% more unique information than teams without information boards (Rentsch, et al., 2014). Teams receiving handouts of each member's skills made 29% fewer mistakes, and recalled 36% more information about other's roles, in comparison to teams that did not use such maps (Moreland & Myaskovsky, 2000).

8.4.2 STRATEGY 2: TRAIN TEAM MEMBERS IN AREAS OTHER THAN THEIR SPECIALTY

Training team members in roles outside of their own job position is known as *cross-training.* Cross-training is a team training approach that is widely used in fields such as the military and has shown considerable benefits in developing SKUE and improving team performance (Cannon-Bowers, Salas, Blickensderfer, & Bowers, 1998). There are three different methods of cross-training (Cannon-Bowers, et al., 1998). Each of these methods can be used within or between teams in CSIRTs.

Lecture/Presentation

The first form of cross-training involves communicating, or presenting to others, aspects of your knowledge or your functional roles and responsibilities (Cannon-Bowers, et al., 1998). This can take the form of a weekly, bi-weekly, or monthly meeting and can

> **"We also encourage the analysts to cross-train. What we call cross-pollination. And we have our first series of analysts' presentations.... We give them a huge list of things they can choose from. Is it sequel injections, cross-eyed scripting, is it buffer overflows, is it S cell reception, and so on? And then they have to give a presentation to the whole group and basically train us on what it is. And we try to do that once a quarter."**
>
> **~ CSIRT Member**

> They just kind of shadow him when the SOC rotates to the CSIRT for a period of time. For example, the engineer sits on the main [floor], and the level one analyst sits behind him and watches it. So I did it two hours every two weeks.
>
> ~ CSIRT Member

involve presentations by one or several team members. Such presentations should occur especially after completion of new projects. When team members (or teams) gain knowledge by working on new types of projects or incidents, passing such information on to the rest of the CSIRT keeps SKUE fully updated. Also, after-action reviews that occur following major events can facilitate team learning contributing to growth of SKUE (see Chapter 11, "Continuous Learning in Incident Response").

Presentations can be designed around one or more of the following areas:

- An illustration of what the individual knows about the topic area;
- How the individual accomplishes tasks and roles in his/her job;
- Descriptions of concepts, ideas, tools, and software that might be new to other team members;
- New strategies and solutions learned from other formal training; and/or
- An overview of a new project a team member has been working on.

In an MTS, such presentations can include the knowledge, purpose, and expertise of different component teams.

Job Shadowing

Team members, particularly novice members, can acquire new knowledge by shadowing other experienced members to learn what they do, what their unique areas of expertise are, and what approaches they take to particular kinds of problems. This "hands-on" form of cross-training is called job shadowing (similar to positional modeling; Cannon-Bowers, et al., 1998). Based on feasibility, CSIRT members can shadow jobs of members within their team or of other teams with whom they might work (e.g., a new member of the incident response team shadowing an experienced member of the forensics or threat intelligence team). Job shadowing allows greater SKUE as team members see the actual functions that other members perform. They can visually understand the motions that other members go through in their daily jobs and understand the constraints they may operate under. This approach to SKUE development also allows members from different teams to communicate and collaborate more effectively, as they "understand one another's language."

> We will encourage them to work throughout the different areas of security so that they can also experience some of the other teams and get an idea of where they want their career paths to go.
>
> ~CSIRT Manager

To implement this strategy effectively, CSIRT managers should:

- Require new members to observe a certain number of experienced members performing their jobs.
- Urge experienced members to act as informal mentors and coaches, explaining how they approach particular problems.
- On a regular basis, encourage members to observe behaviors of other team members for different kinds of problems and incidents so that all members see a full range of expertise possessed by the entire team.
- Use incidents that are escalated as "teachable moments," such that senior analysts instruct junior analysts on how to handle such incidents in the future.

In a CSIRT MTS, such job shadowing can extend to embedding an individual within another team. Indeed, in some of our focus group interviews with CSIRT managers, managers indicated use of these approaches to help their teams understand each other and collaborate better.

Position Rotation

The final form of cross-training, which is more indirectly related to SKUE, is position rotation. Position rotation refers to having individuals temporarily assume the roles of other team members in order to gain better insight into the kinds of issues and problems they confront (Cannon-Bowers, et al., 1998). As with job shadowing, more experienced team members should act as informal mentors and coaches, explaining how they approach particular problems to team members who are (temporarily) assuming their jobs.

Through position rotation, CSIRT members are given the opportunity not only to learn more about others' responsibilities and expertise, but also advance necessary skills needed to perform well at their own position. Position rotation gives the deepest understanding of another CSIRT member's role.

Position rotation is the most resource intensive cross-training method to implement, as it requires a greater amount of time, flexibility, and room for error. This strategy is recommended for CSIRTs who have a need for members who can perform multiple different roles on demand. Smaller CSIRTs who must collapse several team functions across individuals may particularly benefit from this strategy. CSIRT managers can supplement the first two types of cross-training with position rotation to ensure team members are better trained to step into another's role.

To implement this strategy, CSIRT managers should meet the following conditions:

- Only a small fraction of members should be allowed to rotate positions, while keeping the majority of members performing their core tasks;
- Assumed roles should be in a related field and a moderate "stretch" for individuals (rotating someone to a position that is too challenging can be detrimental to confidence and result in costly errors for the CSIRT); and
- More experienced members should be available to guide individuals that are assuming their role to ensure that costly mistakes are not made that negatively affect CSIRT performance.

Effectiveness Evidence:

Research has supported the effectiveness of these cross-training strategies. The following conclusions are from several studies with several different types of teams:

- Teams that sought and gained information about each member's responsibilities in relation to their own responsibilities were able to increase SKUE by 12% (Pearsall, Ellis & Bell, 2010).
- Learning about and practicing other roles accounted for 19% of knowledge of other team member's roles (Gorman, Cooke & Amazeen, 2010).
- Observing others perform their roles led to 39% more knowledge of those roles than those who did not observe others (Smith-Jentsch, Salas, & Baker, 1996).
- Training team members how to perform a task led to 66% higher SKUE when they were all trained as a group and could see one anothers' roles, compared to training individuals to perform their roles independently (Moreland & Myaskovsky, 2000).
- Practicing other team members roles accounted for an increase of 23% in members' teamwork knowledge (Gorman, Cooke, & Amazeen, 2010).
- Position rotation also significantly improved teamwork behaviors by 11%, and the extent to which team members volunteered information by 41% (Volpe, Cannon-Bowers, Salas, & Spector, 1996).
- Position rotation decreased time needed for members to access information by nearly 50% (Cannon-Bowers, et al., 1998).

> **"Because we have one guy that we took from [another group], an extremely talented analyst. And he right now is working with the other analysts to teach them about application level coding.... that helps give them a more well-rounded approach. That's also why we change shifts every three months, is so they experience the different analysts, and they can all benefit from the different skills."**
>
> **~CSIRT Leader**

8.5 Summary

The findings from our project focus groups and surveys indicated that SKUE was quite important for collaboration in incident response. Along with trust and other drivers of CSIRT performance such as communication (Chapter 5, "Communication Effectiveness in Incident Response") and information sharing (Chapter 6, "Information Sharing Effectiveness in Incident Response"), knowing what others members across component teams know quickens the incident response process, including the identification and mitigation of threats. In this chapter, we described strategies that managers and leaders can use to increase SKUE within and between teams. Leaders of effective CSIRTs have suggested that these strategies were important to them for shaping well-rounded teams and team members.

References

Austin, J. R. (2003). Transactive memory in organizational groups: The effects of content, consensus, specialization, and accuracy on group performance. *Journal of Applied Psychology, 88*, 866-878.

Cannon-Bowers, J. A., Salas, E., Blickensderfer, E., & Bowers, C. A. (1998). The impact of cross-training and workload on team functioning: A replication and extension of initial findings. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 40*, 92-101.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business Press.

Gorman, J. C., Cooke, N. J., & Amazeen, P. G. (2010). Training adaptive teams. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 52*, 295–307.

Moreland, R. L., & Myaskovsky, L. (2000). Exploring the performance benefits of group training: Transactive memory or improved communication? *Organizational Behavior and Human Decision Processes, 82*, 117-133.

Nemeth, C., O'Connor, M., Klock, P. A., & Cook, R. (2006). Discovering healthcare cognition: the use of cognitive artifacts to reveal cognitive work. *Organization Studies, 27*, 1011-1035.

Pearsall, M. J., Ellis, A. P., & Bell, B. S. (2010). Building the infrastructure: The effects of role identification behaviors on team cognition development and performance. *Journal of Applied Psychology, 95*, 192-200.

Rentsch, J. R., Delise, L. A., Salas, E., & Letsky, M. P. (2010). Facilitating knowledge building in teams: can a new team training strategy help?. *Small Group Research, 41*, 505–523.

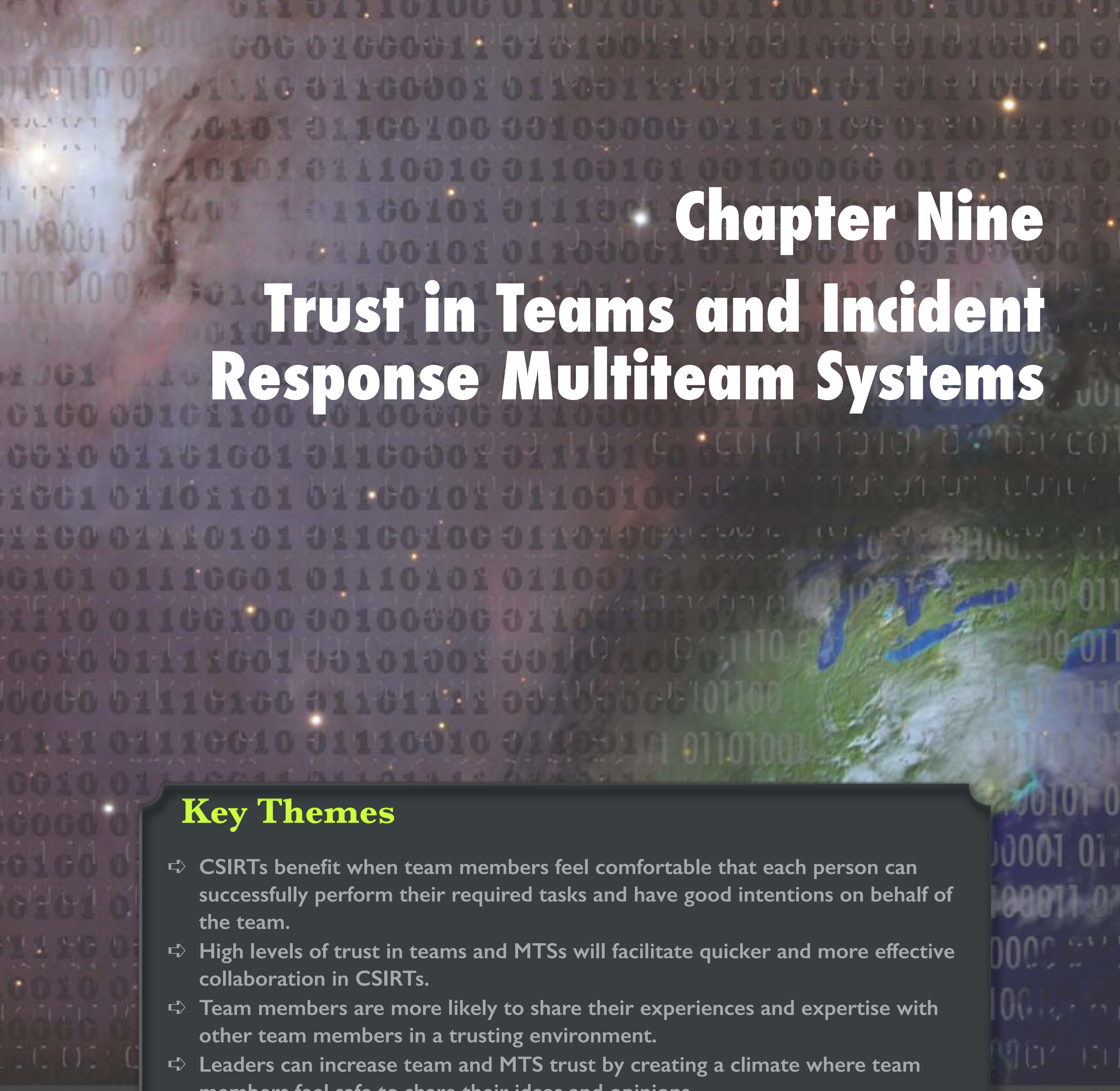
Rentsch, J. R., Delise, L. A., Mello, A. L., & Staniewicz, M. J. (2014). The integrative team knowledge building training strategy in distributed problem-solving teams. *Small Group Research, 45*, 568-591.

Schreiber, M., & Engelmann, T. (2010). Knowledge and information awareness for initiating transactive memory system processes of computer-supported collaborating ad hoc groups. *Computers in Human Behavior, 26(6)*, 1701-1709.

Smith-Jentsch, K. A., Salas, E., & Baker, D. P. (1996). Training team performance-related assertiveness. *Personnel Psychology, 49*, 909-936.

Volpe, C. E., Cannon-Bowers, J. A., Salas, E., & Spector, P. E. (1996). The impact of cross-training on team functioning: An empirical investigation. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 38*, 87-100.

Wegner, D. M. (1986). Transactive memory: A contemporary analysis of the group mind. In B. Mulleb & G. R. Goethals (Eds.), *Theories of group behavior* (pp. 185-205). New York: Springer-Verlag.



Chapter Nine

Trust in Teams and Incident Response Multiteam Systems

Key Themes

- CSIRTs benefit when team members feel comfortable that each person can successfully perform their required tasks and have good intentions on behalf of the team.
- High levels of trust in teams and MTSs will facilitate quicker and more effective collaboration in CSIRTs.
- Team members are more likely to share their experiences and expertise with other team members in a trusting environment.
- Leaders can increase team and MTS trust by creating a climate where team members feel safe to share their ideas and opinions.

> ***“Trust can be one of the biggest obstacles to enhanced and effective communication between CSIRTs but also between CSIRTs and other stakeholders. Lack of trust between stakeholders can lead even to lack of sharing security incident information.”***
>
> ~ Bada, Creese, Goldsmith, Mitchell, & Phillips, 2014, p. 14

Contents

9.0 Introduction

Trust between members in a CSIRT is one of the most important factors for successful collaboration in incident response. Indeed, team and multiteam system (MTS) trust are among the key metrics for determining overall CSIRT performance and effectiveness (see Chapter 3 "Measuring and Evaluating CSIRT Performance"). Much of collaborative problem-solving (CPS) relies on the perception that team members can be trusted to keep their word, perform their duties successfully, and maintain good intentions (Cook & Wall, 1980). Likewise, information sharing and collaborative problem-solving between teams and organizations rests firmly on perceived levels of trust (Bada, Creese, Goldsmith, Mitchell, & Phillips, 2014). Trust becomes especially important for CSIRTs in high-severity situations where threat mitigation is contingent upon coordination of the actions of all team members and there is little time to question the choices and actions of other members (Kozlowski & Ilgen 2006).

9.1 Assessing Team Trust

A The following assessment exercise is designed to provide managers with a diagnostic tool in order to evaluate how well the CSIRT, inidividuals, or component teams within the CSIRT MTS trust one another. This will help determine the social maturity of the CSIRT (See Chapter 2, "The Social Maturity of CSIRTs and Multiteam Systems," for additional information). Based on the responses to this assessment exercise, managers can determine whether they would benefit from the strategies offered in this chapter. Managers should consider the time and resources required to implement these strategies relative to the need for improvement.

Assess how your CSIRT is functioning in this area by responding to the assessment exercise on a 1-5 scale where 1= Strongly Disagree, 2= Disagree, 3= Neither Agree nor Disagree, 4= Agree, 5= Strongly Agree.

GO TO PAGE 154 FOR
STRATEGIES FOR CSIRT MANAGERS

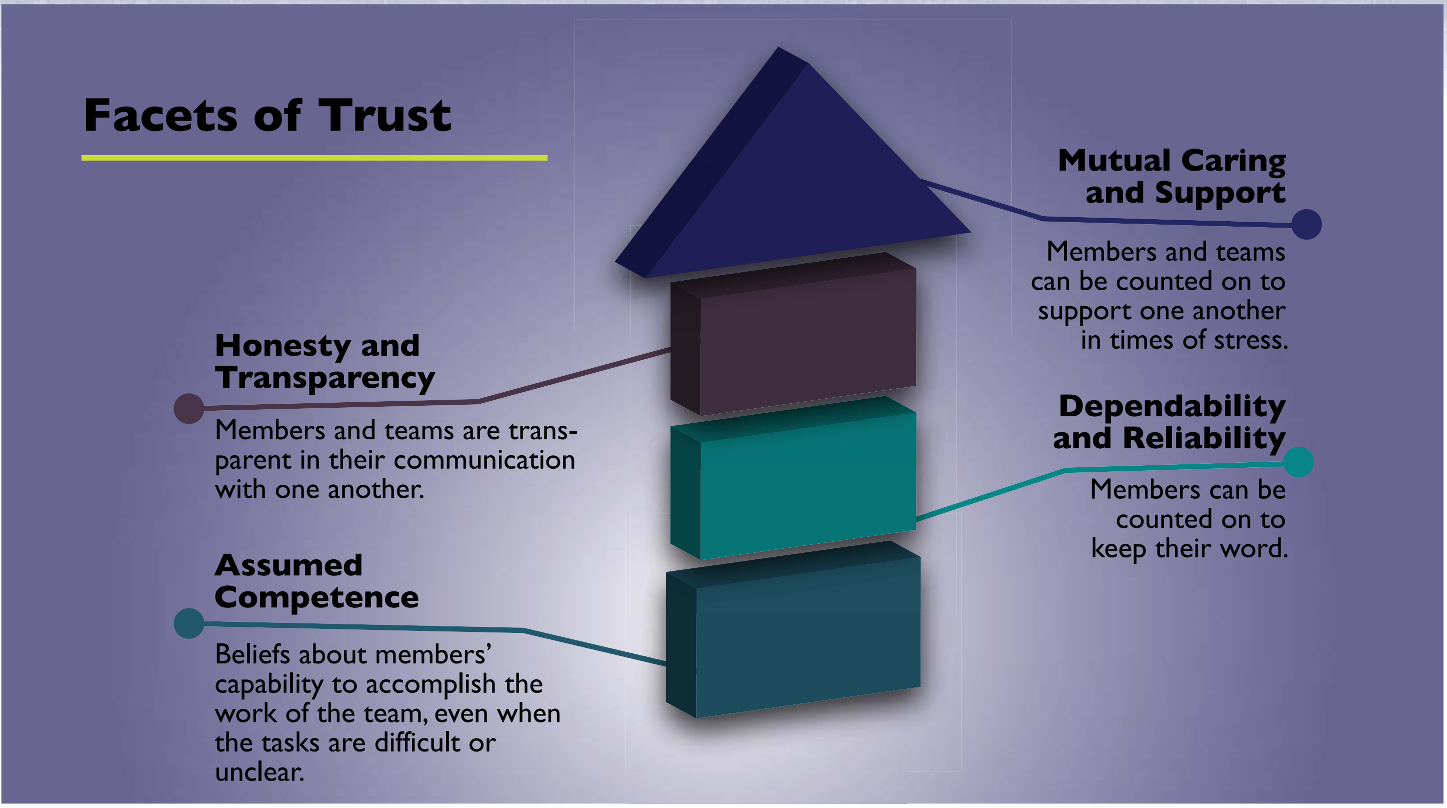
9.2 Background

Organizational scientists have defined the following elements of team trust (see Figure 1) (Bromily & Harris, 2006; Cook & Wall, 1980; Mayer, Davis, & Schoorman, 1995; McAllister, 1995; Zaccaro, Weis, Hilton, & Jeffries, 2011):

1. Assumptions of individual and team competence – beliefs about members' capabilities to accomplish the work of the team, even when the tasks are difficult or unclear;
2. Dependability and reliability – members can be counted on to keep their word;
3. Honesty and openness in communication - members and teams are transparent in their communication with one another; and
4. Mutual caring and support – members and teams can be counted on to provide support in times of stress.

ASSESSMENT EXERCISE

1. My team members feel confident about the competence of other members.
2. My team members feel comfortable relying on each other when resolving tough incidents.
3. My team members feel comfortable admitting mistakes or seeking advice without worrying about being judged or evaluated.
4. My team members share learning opportunities with other members.
5. My team members talk freely with each other about problems they are having resolving incidents.
6. My team members bring up tough problems and issues with each other.
7. Members of my team manage differences of opinion without creating tension.
8. Members of my team resolve disagreements about incident mitigation.
9. Members of my team are comfortable having debates about different approaches to incident mitigation.
10. Tension and anger are well managed among members of my team.
11. My team feels confident about the competence of other teams in a CSIRT MTS.
12. My team members feel comfortable relying on other teams in the CSIRT MTS when resolving tough incidents.
13. My team members share learning opportunities with members of other teams in the CSIRT MTS.
14. Members of my team talk freely with members from other teams in the CSIRT MTS about problems they are having resolving incidents.
15. Team members bring up other tough problems and issues with members of other teams in the CSIRT MTS.
16. My team manages differences of opinion with other teams in the CSIRT MTS without creating tension.
17. Tension and anger are managed well between teams in my CSIRT MTS.



Facets of Trust

Mutual Caring and Support
Members and teams can be counted on to support one another in times of stress.

Honesty and Transparency
Members and teams are transparent in their communication with one another.

Dependability and Reliability
Members can be counted on to keep their word.

Assumed Competence
Beliefs about members' capability to accomplish the work of the team, even when the tasks are difficult or unclear.

Figure 9.1 Facets of Trust (Sources: Bromily & Harris, 2006; Cook & Wall, 1980; Mayer, Davis, & Schoorman, 1995; McAllister, 1995)

As suggested in Figure 1, trust in teams can range in levels of intensity (Zaccaro, et al., 2011). Assumed competency reflects the basic level of quick forming trust among team members. However, as members experience greater numbers of successful experiences, such trust grows to include expectations of dependability and reliability. Further interactions that fulfill such expectations promote inferences of honesty and transparency. Finally, as team members experience repeated stress episodes and learn they can count on one another, deep trust, based on mutual caring and support, develops. A key task for CSIRT managers is to facilitate this progression by first developing quick trust among team members, and then creating the conditions for deeper levels of trust.

> **“A successful performance to me is doing what you promised and in combination with doing what is your responsibility. So in an incident environment you have a lot of work that you cannot anticipate but you can still make agreements to your team members about other actions you are going to carry out. So if you promise to do something, I think that people should stick to that promise. If you have a situation that things change, you communicate about it. I think it is most important in any organization.”**
>
> CSIRT Member

For CSIRTs, trust can exist at multiple levels, including:

- Trust between CSIRT members
- Trust between CSIRT leaders and subordinates
- Trust between teams in an MTS
- Trust between organizations

While the facets of trusts should apply at each of these levels, structural and institutional barriers can impair development of deeper levels of trust. Different teams in an MTS or elsewhere in an organization may have different missions and functions that can produce inter-team conflict, reducing perceptions of transparency and mutual caring (see Chapter 2, “The Social Maturity of CSIRTs and Multiteam Systems”). Moreover, different organizations may have policies in place that mandate careful disclosure and restrict other key types of information from being shared outside of the organization. Thus, the formation of deeper levels of trust becomes more difficult with others outside of the team.

We have described two types of trust that can develop depending on *how much* interaction members have with one another. Swift, or quick, trust develops after a series of initial and limited interactions. Deep trust emerges from a sustained pattern of interactions. Managers can use a range of strategies described later in this chapter to develop both forms of trust.

> **“But yeah, trustworthiness of information, especially information that's contradictory to other things you're reading, yeah, that's an important question and I will definitely trust it more if it comes from a trusted source.”**
>
> **~ CSIRT Member**

9.2.1 SWIFT TRUST

Swift trust refers to the initial level of trust that forms in teams in which members have little or no experience working together (Meyerson, Weick, & Kramer, 1996). Such trust formation becomes particularly critical in early stages of new CSIRT formation, when there is a high need to begin acting as a team immediately and little time to engage in longer-term trust building interactions. Swift trust formation also needs to occur in ad hoc CSIRTs where unfamiliar members come together for a short time to resolve a specific incident. Likewise, organizational scientists have noted that swift trust is often particularly necessary in both virtual and global teams (Crisp & Javenpaa, 2013; Germain, & McGuire, 2014).

Swift trust formation is important in newly formed, ad hoc, virtual, or global CSIRTs because members generally have had few opportunities to gain sufficient knowledge of each member's background, experiences, and areas of expertise. When CSIRTs are dispersed or composed of members and teams in different physical spaces (or working in different time zones), the lack of face-to-face interaction inhibits acquisition of such knowledge (Germain, & McGuire, 2014). This difficulty is compounded when virtual teams also include members from different countries, especially those in which cultural values constrain exchange of personal or background information (Zakaria & Yusof, 2015). The lack of knowledge about members' backgrounds and expertise impairs the development of competency perceptions. When members share certain experiences or skills, they perceive one another to be competent and capable of doing their jobs. In later phases of teamwork, initial judgments based on knowledge of backgrounds or competence are confirmed or revised as members interact more closely. Likewise, repeated successful interactions provide additional information about dependability and reliability, particularly about members' tendencies to keep their word. At this point, deeper trust begins to develop (Adams, Waldherr, Sartori & Thomson, 2007). Thus, a key task for managers in newly formed, ad hoc, virtual, and/or global CSIRTs is to ensure that members share information about their backgrounds, past performances, and functional expertise. Moreover, they need to set very clear expectations and norms about members adhering to their word and following up on promised actions.

> **“Trust is key. You really need to see people and talk to people to earn trust, and you also get a feeling of what kind of organization they actually work for. So if you can trust them if they come to you, and that's why we invest a lot in community outreach.”**
>
> **~ CSIRT Member**

9.2.2 DEEP TRUST

When team members have had enough interactions to make accurate judgments about the competence and dependability of others on the team, then deeper forms of trust begin to form. Deep trust is a greater level of trust that forms when team members communicate frequently, perform their roles successfully, and demonstrate their good intentions on behalf of the team (McAllister, 1995). Additional and more frequent interactions begin to provide information about the honesty and openness of fellow members. When interactions occur in demanding contexts, and members engage in "back-up behaviors" to help others cope with increased stress and workloads, then trust, in terms of mutual support and caring, emerges. Back-up behavior refers to a team member's actions to help out other members; these actions can take the form of coaching others, assisting them on the task, and, when necessary, stepping in and assuming responsibility for task accomplishment (Marks, Mathieu, & Zaccaro, 2001). When such behaviors occur in a psychologically safe environment (see Section 9.2.3), members learn they can depend on the help and care of their fellow members in stressful circumstances. Likewise, greater openness and honesty among team members, as well as demonstrations of caring and support, create a team climate where team members become more comfortable in giving advice, seeking and offering help, sharing experiences, and admitting mistakes (Evans, Cianciolo, Hunter, & Pierce, 2010).

9.2.3 TEAM CLIMATE

A trusting climate in a team, MTS, or organization promotes what organizational scientists refer to as psychological safety (Edmondson, 1999). When teams are high in psychological safety, members share the belief that they will not be ridiculed for offering unusual and novel suggestions or ideas. Thus, one of the hallmarks of psychological safety is that it facilitates the willingness among team members to offer unique ideas and advice about team problems (Edmondson & Lei, 2014). Psychological safety

> **“The problem [or] the challenge is to have trust within a group. And you do that, I do that by 1) setting an example. What do I do myself? And 2) looking each other in the eyes and talk about things that are often there or should be there.”**
>
> **~ CSIRT Member**

also enables team members to feel comfortable admitting mistakes without the fear that the team will react negatively (Edmondson, 1999), a major factor in fostering team learning (See Chapter 11, “Continuous Learning in Incident Response”). Open dialogue about mistakes helps teams learn proper actions for future similar incidents. Psychological safety creates the space for such dialogue. Accordingly, for both collaborative problem-solving and team learning, a key task for CSIRT managers is to use particular strategies and leadership behaviors to foster a strong sense of psychological safety in their team (See Chapter 7, "Collaborative Problem-Solving in Incident Response," and Chapters 11, "Continuous Learning in Incident Response").

Conflict and Trust

Team trust is also a key component in conflict management. As we noted in Chapter 7, “Collaborative Problem-Solving in Incident Response,” collaborative problem-solving in knowledge work teams entails exchange and evaluation of ideas. However, research has shown that without trust, a debate about ideas can become more toxic and turn into high interpersonal conflict in the team or MTS (Simons & Peterson, 2000). Such conflict can further damage any existing trust ties. Creating a psychologically safe environment for such debates can help prevent this from happening. However, when a debate about ideas does become heated and begins to be more destructive to the team, managers should engage in the following actions (Gebelein, et al., 2010; Eunson, 2007; Rahim, 2015; Raines, 2012):

- Insist on civil tones and exchanges. If team members are getting angry with one another in a debate, stop the discussion and call a “time-out” until everyone cools down. If necessary, talk to the individual members involved to redirect their energy away from attacking the other members.
- Help the team reframe the argument, by reminding them that critiquing an idea is not the same as criticizing the person who offers the idea. Bring the focus of the discussion to the task and away from particular persons.
- Focus the discussion on the central and common goal – on what is important for the team as a whole.
- Avoid competition among team members – this is *collaborative* problem-solving, not *competitive* problem-solving.
- Help identify information gaps. For example, ask dissenting members, “you feel strongly about X, can you tell me why?”
- When members are arguing from very different points of view, ask them to take on and consider the issue from the other member’s perspective.
- Ensure that members are actively listening to one another instead of forming their own responses while the others are talking (stop “yes, but…” dialogues). Ask members to summarize the points of others in the discussion.
- Set rules on how teams will reach decisions (supermajority of 2/3 or 3/4 of members agreeing; majority rule). Avoid full consensus rules, if possible. Make sure all sides are fully heard before implementing decision rule.

> **“…first, the team is known within the organization and the team actually knows other teams within the organization. That is the first thing. Another thing is that the subjects that we work on, people are afraid. People do not want to share, so another aspect is that you need to be personal...It is very important that people actually know who you are.”**
>
> **~ CSIRT Member**

These strategies can support a psychologically safe environment and prevent a disagreement about ideas from blowing up into a full-scale and destructive argument in the team. For MTSs, these strategies can be used among teams working together. When the debate occurs among representatives of the teams (instead of among all members of the MTS), they need to ensure that they keep their teams informed of the discussions and manage any reactions from the team. If possible, they should bring more than one key representative from the different teams to MTS discussions about conflicting ideas.

9.2.4 TRUST BETWEEN TEAMS, ORGANIZATIONS AND EXTERNAL PARTIES

The implications of trust (or the lack thereof) extend to the interactions between teams, organizations, and external stakeholders. Indeed, “trust can be one of the biggest obstacles to enhanced and effective communication between CSIRTs but also between CSIRTs and other stakeholders” (Bada, et al., 2014, p. 14). Inter-organizational trust is a collectively held trust belief toward another organization and develops from two sources: (1) each organization’s reputation, and (2) the degree of similarity in operational values and attitudes across the cooperating organizations (Ybarra & Turk, 2009).

The foundations of inter-team and inter-organization trust are the same ones noted in Figure 1 for team trust:

- Assumption that another team or organization has the competence to accomplish its part of a shared mission;
- Belief that another team or organization will keep its word and follow through on promised actions;
- Perception that another team or organization is being transparent in its communications and actions; and
- Belief that another team or organization will provide support for your team and organization in stressful or threatening circumstances.

When these conditions are met, information sharing between teams and organizations can be quite fluid and frequent (See Chapter 6 on “Information Sharing Effectiveness in Incident

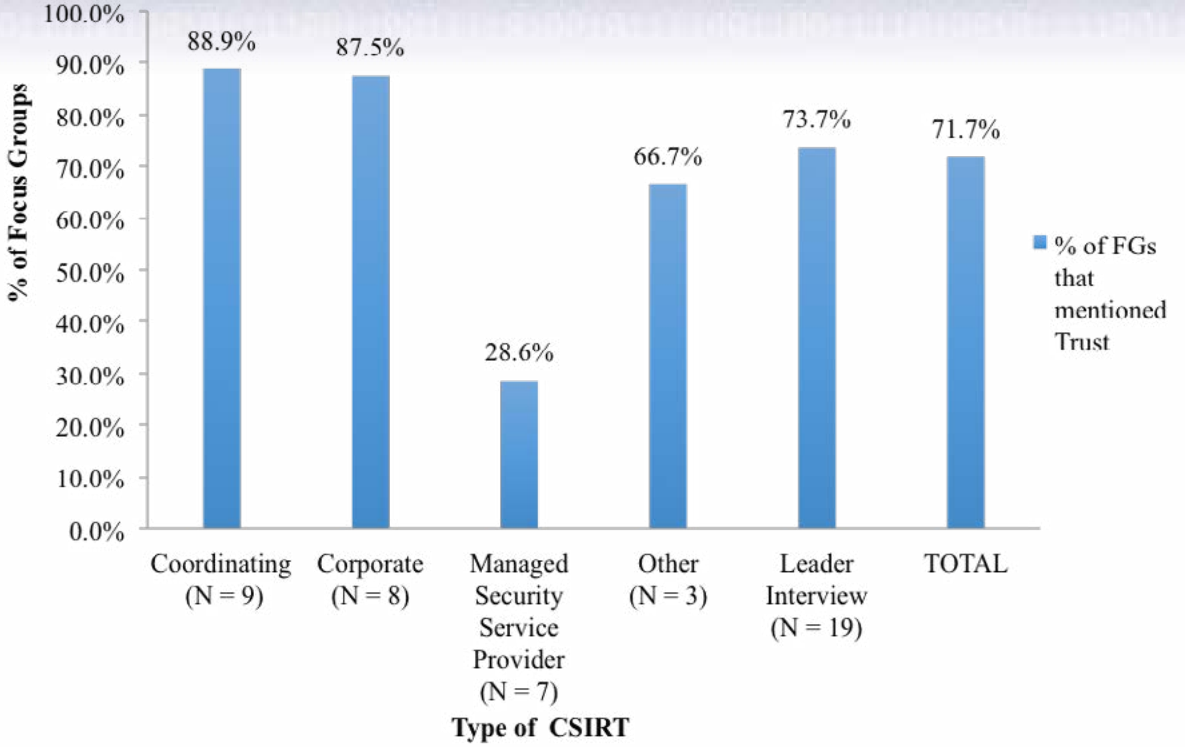


Figure 9.2 Focus Group Support for Trust by CSIRT Type.

Response" for more information). However, several common barriers to these conditions exist that often prevent necessary levels of trust between teams and organizations (Ruefle, Dorofee, Mundie, Householder, & Murray, 2014). First, teams and organizations rarely interact enough to gain assumptions of competence, or, particularly, a sense of how well other companies can safeguard and securely handle sensitive information. Second, competitive pressures create mixed motives that may interfere with promises to share information. While companies may have a common goal for information sharing, they each may have other goals that conflict with such cooperation. Third, such pressures, as well as a fear of negative publicity, may cause other teams and organizations to be less transparent and open in their information sharing. Likewise, organizational regulatory policies may prevent full disclosure of certain kinds of information. Finally, a natural tendency toward self-preservation reinforced by internal pressures to "put one's team or organization first" can reduce inter-team and inter-organizational support during stressful or threatening circumstances.

Organizations in cybersecurity have developed a number of control mechanisms to facilitate trustworthy connections and information sharing. These include Trusted Introducer (Dufková, 2013; Skierka, Morgus, Hohmann, & Maurer, 2015), identity assurance programs (National Academy of Science & The Royal Society, 2015), trustworthiness ratings, and the Authentication – Authorization – Accountability model (MACCSA, 2013). These strategies may be helpful in establishing competence and reliability facets of trust. However, organizational scientists have argued that such compliance mechanisms are "weak, impersonal substitutes" for the levels of deeper trust necessary for collaborative problem-solving between teams and organizations (Mayer, et al., 1995, p. 710). Instead, these mechanisms, which are useful for swift trust, should be augmented with strategies that establish greater familiarity and ties with individuals across teams and organizations (Bada, et al., 2014).

9.3 Project Findings

Trust and psychological safety were mentioned as critical for CSIRT effectiveness in 72% (33 of 46) of our interviews with CSIRT members and leaders. Likewise, in a survey of the top attributes needed for CSIRT effectiveness, 97.6% of cybersecurity experts reported that the extent to which team members can be counted on to follow through on promises and complete tasks was particularly important for CSIRT performance. These data indicate that CSIRT members consider trust to be an import-

> “***Interviewer***: How do you get to know what everyone knows?
> ***CSIRT Member***: We have it written down on paper explicitly.
> ***Interviewer***: You have explicitly what each person knows?
> ***CSIRT Member***: Yeah, well, what their specialties and areas.”

ant factor for threat mitigation and incident resolution.

Figure 9.2 shows the percentage of analysts and managers in our focus group interviews that identified trust as an important attribute in their CSIRTs. These are aggregated by type of CSIRT. Interestingly, CSIRT managers and leaders across all different types of CSIRTs identified trust as important to CSIRT effectiveness with the notable exception of those in fee-based services provided by managed security service providers. This finding may reflect that managed security service providers are contracted to provide a limited set of functions that do not include the same need for trusted relationships as other CSIRT types, or, in contrast, may reflect a deficiency by such services to emphasize the importance of trust. Much more data would need to be collected to understand the reason for this particular finding and to see if this finding would generalize to other managed security service providers that were not included in this research. However, most managers across different CSIRT types can benefit from the recommendations presented in the next section.

9.4 Developing Team Trust

In this section we provide exercises and recommendations related to building trust in teams, MTSs, and between organizations. Please use the assessment exercise at the beginning of this chapter to evaluate the level of trust in your CSIRT, and to help you determine the best strategies to improve your team.

9.4.1. STRATEGY 1: PROVIDE STRUCTURED OPPORTUNITIES FOR CSIRT MEMBERS TO LEARN ABOUT THE EXPERTISE, EXPERIENCES, AND FUNCTIONAL BACKGROUNDS OF OTHER MEMBERS

When CSIRTs are newly formed, or when members have not previously worked together, building perceptions of shared competence is an important first step in developing team trust. Disclosing unique skills and experiences helps to demonstrate that all team members are competent in their roles. In Chapter 8, “Shared Knowledge of Unique Expertise,“ we presented several strategies for facilitating the sharing of unique expertise (SKUE) among CSIRT members. These include use of (a) information boards, (b) knowledge maps and banks, and (c) cross-training in the form of member lectures/presentations. While each of these strategies can boost the development of SKUE in teams, they also facilitate trust development in terms of perceived competence. The use of information boards and knowledge banks are particularly effective when new or ad hoc CSIRTs have members who are geographically and globally dispersed.

Recommendations for Use:

Managers should encourage team members to engage in frequent interactions and informal conversations in which they exchange information about the following: backgrounds, work experiences, and (some) personal information that emphasizes common interests. This information exchange gives each person the knowledge they need to create perceptions of trust in their teammates. These interactions also help create a team identity. From these interactions, teammates should be able to gather relevant information regarding teammates’ work-related skills, abilities, motivations, and habits (Jarvenpaa, Knoll, & Leidner, 1998).

Effectiveness Evidence

Research has demonstrated the effectiveness of providing background information about members for developing swift trust. In a military setting, when team members received information on other team members’ backgrounds (e.g., military unit) during a pre-brief (See Chapter 7, “Collaborative Problem-Solving in Incident Response,” for a definition and more information on pre-briefing), their perception of those members’ trustworthiness was 8% higher when backgrounds were similar than those who received no information (Adams, et al., 2007). Overall team trust was also 8% higher (Adams, et al., 2007). In another study of team members working in global virtual teams, providing members with information of each other’s backgrounds contributed to perceptions of competence by 14% while also contributing to positive impressions of member integrity by 9% (Jarvenpaa et al., 1998).

9.4.2. STRATEGY 2: ESTABLISH CLEAR INDIVIDUAL AND TEAM GOALS, ROLES, AND PERFORMANCE STANDARDS

A related strategy for developing perceptions of shared competence is for managers to set unambiguous team goals and ensure that members have a clear sense of these goals, their roles in meeting these goals, and the performance standards that indicate goal accomplishment. This strategy can also strengthen the basis for increased dependability and reliability in the team, as members become more familiar with the tasks other members are expected to accomplish. Making each member’s role visible to the rest of the team helps create a shared understanding of how the team must work together. Setting goals for individuals and for the entire team increases the perception that individual members must rely on one another to accomplish the teams’ goal. Sharing a common goal with team members that are viewed as dependable increases the team’s motivation to achieve these goals. Swift trust can then evolve into deeper trust as the team continues to interact effectively (Klein et al., 2009). This same strategy can be used between teams in an MTS (please see Chapter 2, “The Social Maturity of CSIRTs and Multiteam Systems,” on emphasizing distal goal commitment in MTSs).

Recommendations for Use:

CSIRT managers can use the team chartering strategy described in Chapter 5, “Communication Effectiveness in Incident Response,” and the pre-briefing strategy described in Chapter 7, “Collaborative Problem-Solving in Incident Response,” to establish member and team roles and to set team and MTS goals. The following guidelines are useful in setting and monitoring goals (adapted from Senecal, Loughead & Bloom, 2008):

- Define the team goals for a specific period of time (e.g. monthly). Ask each member to provide a list of team goals, actively discuss these goals and collectively select the ones that team members agree on as important.

- Based on the team goals, instruct each member to specify their own individual goals. Make sure that team members align their individual goals with shared team goals.
- Meet with the team members on a regular basis to remind them of goals, evaluate progress toward goals, and provide feedback. When giving goal-setting feedback, leaders should:
    - Instruct members to focus on improving skills and gaining competence when setting individual as well as team goals.
    - Ensure that feedback is provided with the intent of developing team members and helping them grow, not providing performance reviews or promotion decisions.
    - Encourage members to learn from mistakes and build on each other's ideas to develop strategies for improvement.

Effectiveness Evidence:

Defining and understanding team member roles has been shown to increase swift trust in teams and contributes up to 12% to team effectiveness (Klein et al., 2009). When teams define and generate shared team goals before performing tasks, team cohesion, a factor in team trust, improves by as much as 70%, and the degree to which members perceive a collaborative and trusting climate in the team improves by 88% (Huang, Wei, Watson & Tan, 2002). In virtual teams, such activities improves members' perceptions of collaborative and trusting climate by 111% (Huang, et al., 2002).

9.4.3 STRATEGY 3: ESTABLISH NORMS FOR COMMUNICATION TRANSPARENCY IN TEAMS AND MTSs

The first two management strategies in this section help establish swift trust and establish the basis for further trust development. Deeper levels of trust begin to occur when managers create and enforce a climate for communication transparency. This climate begins with the manager's own transparency. Team and MTS members look to the leader for expectations of how they should behave (Tyler & Lind, 1992). If CSIRT managers model openness and honesty in their communications with others, then their subordinates will be more likely to do the same. However, if managers engage in careful disclosure when working with the CSIRT, that will create a less transparent climate among their subordinates.

Managers should also enforce a norm for communication transparency by reacting swiftly to violations of this norm. If team members display a reluctance to be open in their interactions with their colleagues, managers should have a "clearing the air" meeting with those particular individuals, with team leads, and, if necessary, with the CSIRT as a whole. The tone of such meetings should be constructive and supportive, with the purpose of addressing issues that are fostering careful disclosure rather than transparency in communications within the team.

> **“'I work to do this. I'm not sure if the policy says I can do this, or I need to do this in this way. Can you help me?' And that's the way things work. And then, also, as sort of a control mechanism, there is the sort of – you can call it a policy incident. Things tend to go wrong in operations, of course. Things tend to go wrong in policy, also, all the time. But I think we have quite an open culture in saying things go wrong.”**
>
> **~CSIRT Leader**

This strategy becomes particularly important when resolving transparency issues in an MTS. CSIRT MTS managers should establish norms for transparency between different teams. When such norms are violated, "clearing the air" meetings can occur with representatives from each team.

Effectiveness Evidence:

When managers are open, their employees feel their manager listens to them, gives fair weight to their ideas, and takes action to address their needs or concerns (Detert & Burris, 2007). Management openness also decreases any perceived power differential between a manager and employee, which creates a psychologically safe climate and allows employees to feel safe bringing up risky ideas. Openness of management has been found to influence the communications of their employees. Manager openness contributed 10% to the open communications employees exhibited toward managers (Detert & Burris, 2007). Manager openness also contributed 18% to perceptions of psychological safety (Detert & Burris, 2007). With members of multinational teams, manager openness contributed 23% to team members' perceptions of psychological safety and 20% to employee open communications directed at the leader (Tröster & van Knippenberg, 2012). It also contributed to 10% of team member commitment (Tröster & van Knippenberg, 2012).

Another benefit of communication openness is that it helps prevent task-related conflict between team members from becoming interpersonal, or relationship-related. Task conflict that becomes personal results in disliking and decreased trust between team members. Communication openness contributes 18% to trust, but, even more importantly, is that communication openness can help prevent both task and relationship conflict from reducing trust in teams (Ayoko & Pekerti, 2008).

9.4.4 STRATEGY 4: UTILIZE MANAGERIAL ACTIONS THAT CREATE A PSYCHOLOGICALLY SAFE CLIMATE IN THE TEAM AND THE MTS

An important element in developing deep trust in CSIRTs is managers creating a psychologically safe climate for helping members generate novel ideas, explore new perspectives, and learn from mistakes. Working in a "zero-defect" environment constrains such contributions and results in less effective CSIRTs. To create a psychologically safe climate, CSIRT managers should ensure that team members feel valued. They should encourage them to generate the novel ideas that are often necessary to resolve unusual incidents. During all problem-solving stages, the leader should include all team members in the process, de-emphasize status differences, and convey appreciation for all team members' ideas (Nembhard & Edmondson, 2006).

Recommendations for Use:

The following tips are recommended for ensuring a psychologically safe climate during the phases of collaborative problem-solving (Edmondson, 1999; Klein et al., 2009; Nembhard & Edmondson, 2006).

- During team discussion, invite all team members to offer opinions, as some might be hesitant to go against the majority.
- Actively try to take on other team members' perspectives (this strategy is also useful when dealing with other teams or other organizations).
- Weight all team members' ideas equally and consider each opinion before coming to a decision (this includes de-emphasizing status differences between team members and between team members and the leader).
- Allow all team members to be involved in decision-making (including choosing a solution).
- Openly discuss errors and mistakes.
- Encourage team members to bring up difficult topics and reward them (e.g. with praise) for offering new solutions or ideas.
- Require and reward team members to disclose important information or experiences that may prevent mistakes and help the team grow as a whole.
- Display non-defensive responses to questions and challenges.
- Ensure all members are present when discussing important information so that everyone remains involved and in the loop (this may require video conferencing with geographically dispersed teams).
- Provide team members with necessary information and resources.

Also, the types of goals that leaders encourage are important for developing a psychologically safe CSIRT climate. In particular, managers should foster learning goals in the CSIRT to create a climate of psychological safety. Learning goals encourage members to perceive errors as opportunities to learn and promote team trust rather than as failures. Thus, they foster greater exploration by CSIRT members and can result in greater learning gains for the team as a whole. Chapter 11, "Continuous Learning in Incident Response," provides additional recommendations on creating a learning climate in CSIRTs.

While these suggestions are provided for team psychological safety, they apply as well to creating safe climates between teams in an MTS. Managers can employ the above tips when members from different teams come together to resolve particular incidents.

> **"We do things like pack bonds, capture the flag training efforts, all hands meetings on Wednesdays. This really gives the analysts a chance to work together, [and] stretch their wings."**
>
> **~CSIRT Leader**

Effectiveness Evidence:

Specific leader behaviors that reflect inclusiveness and appreciation for team member ideas have been found to increase psychological safety by 55% (Nembhard & Edmondson, 2006). Providing team members with adequate support and responding in a non-defensive manner to questions and challenges has been found to contribute 49% and 40%, respectively, to psychological safety (Edmondson, 1999).

Setting learning goals has also been found to facilitate a psychologically safe environment in the team. In one study, setting learning goals improved team psychological safety by an average of 6%, team learning behavior by an average of 8%, and performance output by an average of 16%, when compared to team members focusing just on performance goals (Ashauer & Macan, 2013).

9.4.5 STRATEGY 5: CREATE OPPORTUNITIES FOR BUILDING STRONG SOCIAL CONNECTIONS AMONG CSIRT MEMBERS TO SUPPORT CONFLICT MANAGEMENT

Both swift trust and deep trust emerge from positive social relationships among CSIRT members. Conflict will always occur in CSIRTs. Yet, a manager can minimize the damage to trust that conflict can cause by helping the team develop stronger interpersonal ties early in the team's formation. Such ties can minimize the degree to which disagreements about ideas during collaborative problem-solving.

Recommendations for Use:

Leaders can use the following activities to build stronger social ties and manage interpersonal conflicts in their CSIRTs.

- Provide "ice-breaking" social activities early in the team's formation or as new members join (Abrams, Cross, Lesser, & Levin, 2003);
- Have regular team social activities (e.g., team lunches, gaming activities), especially if teams are not new; and
- Engage the team (or multiple teams in an MTS) in training activities that improve conflict resolution strategies to handle conflict constructively (Stevens & Campion, 1994).

Effectiveness evidence:

Research studies have shown that when teams use conflict management strategies to resolve interpersonal issues or confrontations, overall team trust is 43% higher (Boss & Mcconkie, 1981).

Training activities that specifically focus on improving conflict management have been shown to lead to 13% higher interpersonal trust (Hughes, Rosenbach & Clover, 1983). As Strategy 3 described above, communication openness prevents task and relationship conflict from decreasing trust (Ayoko & Pekerti, 2008). Teams comprised of members who are familiar with each other or are friends with one another have 7% greater perceptions of team trust climate than teams of members who are not familiar with each other. They also have 6% higher perceptions of trustworthiness and display 7% more cooperative behaviors. These differences remain constant across time, from the beginning to the end of a project (Costa, Bijlsma-Frankema & de Jong, 2009). Team cohesion (of which one component is time spent together as a team) contributed 50% to organizational trust (Gilbert & Tang, 1998).

9.4.6 STRATEGY 6: INCREASE EXTERNAL CONNECTIONS AND SOCIAL NETWORKING TO FACILITATE INTER-TEAM AND INTER-ORGANIZATION TRUST

Trust among teams in an MTS can be developed through consistent networking across team boundaries. A similar strategy can build inter-organizational trust by promoting networking across organizational boundaries (Bada, et al., 2014). Indeed, such networking is a key element in enhancing CSIRT maturity (CSIRT Maturity Kit, n.d.). Networking can be done at annual professional meetings, or regularly scheduled meetings among individuals from different organizations who need to work with one another (See also Chapter 11, “Continuous Learning in Incident Response”). Appendix H, "Building Informal CSIRT Networks to Enhance the Indcident Response Process," provides an expanded description of social networking and the role of effective external relationships in CSIRTs. This appendix provides several useful networking strategies.

9.5 Chapter Summary

The CSIRT community has placed a significant emphasis on trust as an important factor for collaboration in incident response, one that was confirmed in our project findings. Trust within teams, between teams, and between organizations has implications for communication, information sharing and all other steps in the collaborative problem-solving process. CSIRT teams with high levels of trust facilitate faster threat mitigation with better, more novel solutions due to the conditions created by team leaders. Leaders and managers can use the strategies in this chapter to foster trust at all levels of the organization. CSIRT Managers should review the material in Chapter 8 on Shared Knowledge of Unique Expertise (SKUE). The recommendations to increase SKUE can also foster swift trust in teams.

References

Abrams, L. C., Cross, R., Lesser, E., & Levin, D. Z. (2003). Nurturing interpersonal trust in knowledge-sharing networks. *The Academy of Management Executive, 17*, 64-77.

Adams, B. D., Waldherr, S., Sartori, J., & Thomson, M. (2007). *Swift trust in distributed ad hoc teams* (No. DRDC-CR-2007-139). Human Systems Inc Guelph (Ontario).

Ashauer, S. A., & Macan, T. (2013). How can leaders foster team learning? Effects of leader-assigned mastery and performance goals and psychological safety. *The Journal of Psychology, 147*, 541-561.

Ayoko, O. B., & Pekerti, A. A. (2008). The mediating and moderating effects of conflict and communication openness on workplace trust. *International Journal of Conflict Management, 19*, 297-318.

Bada, M., Creese, S., Goldsmith, M., Mitchell, C., & Phillips, E. (2014). *Improving the effectiveness of CSIRTs*. Global Cyber Security Capacity Centre. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Improving%20the%20effectiveness%20of%20CSIRTs.pdf

Boss, R. W., & Mcconkie, M. L. (1981). The destructive impact of a positive team-building intervention. *Group & Organization Management, 6*, 45-56.

Bromiley, P., & Harris, J. (2006). Trust, transaction cost economics, and mechanisms. In R. Bachmann & A. Zaheer (Ed.), *Handbook of trust research* (pp. 124-143). Cheltenham, UK, Northampton, MA, USA: Edward Elgar Pub.

Cook, J., & Wall, T. (1980). New work attitude measures of trust, organizational commitment and personal need non-fulfillment. *Journal of Occupational Psychology, 53*, 39-52.

Costa, A. C., Bijlsma-Frankema, K., & de Jong, B. (2009). The role of social capital on trust development and dynamics: implications for cooperation, monitoring and team performance. *Social Science Information, 48*, 199-228.

Crisp, C. B., & Jarvenpaa, S. L. (2013). Swift trust in global virtual teams: Trusting beliefs and normative actions. *Journal of Personnel Psychology, 12*, 45-56.

CSIRT Maturity Kit. (n.d.). Retrieved from https://check.ncsc.nl/static/CSIRT_MK_brochure.pdf

Detert, J. R., & Burris, E. R. (2007). Leadership behavior and employee voice: Is the door really open?. *Academy of Management Journal, 50*, 869-884.

Dufková, A. (2013). *CERT community: Recognition mechanisms and schemes* (ENISA ISBN 978-92-9204-083-3 doi:10.2788/14231).

Edmondson, A. (1999). Psychological safety and learning behavior in work teams. *Administrative science quarterly, 44*, 350-383.

Edmondson, A. C., & Lei, Z. (2014). Psychological safety: The history, renaissance, and future of an interpersonal construct. *Annual Review of Organizational Psychology and Organizational. Behavior, 1*, 23-43.

Eunson, B. (2007). *Conflict management.* Milton, Qld, Australia: John Wiley & Sons Australia, Ltd.

Evans, K. M., Cianciolo, A. T., Hunter, A. E., & Pierce, L. G. (2010). *Modeling interpersonal trust in distributed command and control teams*. Command Performance Research Inc. Champaign IL.

Gebelein, S. H., Nelson-Neuhaus, K. J., Skube, C. J., Lee, D. G., Stevens, L. A., Hellervik, L. W., & Davis, B. L. (2010). *Successful manager's handbook*. Roswell, GA: PreVisor.

Germain, M. L., & McGuire, D. (2014). The role of swift trust in virtual teams and implications for human resource development. *Advances in Developing Human Resources, 16*, 356-370.

Gilbert, J. A., & Tang, T. L. P. (1998). An examination of organizational trust antecedents. *Public Personnel Management, 27*, 321-338.

Huang, W. W., Wei, K. K., Watson, R. T., & Tan, B. C. (2003). Supporting virtual team-building with a GSS: an empirical investigation. *Decision Support Systems, 34*, 359-367.

Hughes, R. L., Rosenbach, W. E., & Clover, W. H. (1983). Team development in an intact, ongoing work group: A quasi-field experiment. *Group & Organization Management, 8*, 161-186.

Jarvenpaa, S. L., Knoll, K., & Leidner, D. E. (1998). Is anybody out there? Antecedents of trust in global virtual teams. *Journal of Management Information Systems, 14*, 29-64.

Klein, C., DiazGranados, D., Salas, E., Le, H., Burke, C. S., Lyons, R., & Goodwin, G. F. (2009). Does team building work?. *Small Group Research, 40*, 181-222.

Kozlowski, S. W., & Ilgen, D. R. (2006). Enhancing the effectiveness of work groups and teams. *Psychological Science in the Public Interest, 7*, 77-124.

MACCSA (2013). *Collaborative Cyber Situational Awareness (CCSA) Information Sharing Framework (ISF.) Released – 20 Nov 2013 (Version 2.4).* Retrieved from https://www.terena.org/mail-archives/refeds/pdfjJz1CRtYC4.pdf

Marks, M. A., Mathieu, J., & Zaccaro, S. J. (2001). A temporally based framework and taxonomy of team processes. *Academy of Management Review, 26*,356-376.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*, 709-734.

McAllister, D. J. (1995). Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal, 38*, 24-59.

Meyerson, D., Weick, K. E., & Kramer, R. M. (1996). Swift *Trust and Temporary Group. In R. Kramer & T. Tyler (Eds.), Trust in organisations: frontiers of theory and research* (pp. 166-195). Thousand Oaks, CA, US: Sage Publications.

National Academy of Science & The Royal Society. (2015). *Cybersecurity dilemmas: Technology, policy, and incentives: Summary of discussions at the 2014 Raymond and Beverly Sackler U.S.-U.K. Scientific Forum*. Washington, DC: The National Academies Press.

Nembhard, I. M., & Edmondson, A. C. (2006). Making it safe: The effects of leader inclusiveness and professional status on psychological safety and improvement efforts in health care teams. *Journal of Organizational Behavior, 27*, 941-966.

Rahim, M. A. (2015). *Managing conflict in organizations*. New Brunswick, NJ: Transaction Publishers.

Raines, Susan S. (2012). *Conflict management for managers: Resolving workplace, client, and policy disputes*. Wiley & Sons.

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer security incident response team development and evolution. *Security & Privacy, IEEE, 12*, 16-26.

Senécal, J., Loughead, T. M., & Bloom, G. A. (2008). A season-long team-building intervention: Examining the effect of team goal setting on cohesion. *Journal of Sport & Exercise Psychology, 30*, 186-199.

Skierka, I., Morgus, R., Hohmann, M., & Maurer, T. (2015). *CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams*. Retrieved from https://static.newamerica.org/attachments/2943-csirt-basics-for-policy-makers/CSIRT%20Basics%20for%20Policy-Makers%20May%202015%20WEB%2009-15.16efa7bcc9e54fe299ba3447a5b7d41e.pdf

Stevens, M. J., & Campion, M. A. (1994). The knowledge, skill, and ability requirements for teamwork: Implications for human resource management. *Journal of Management, 20*, 503-530.

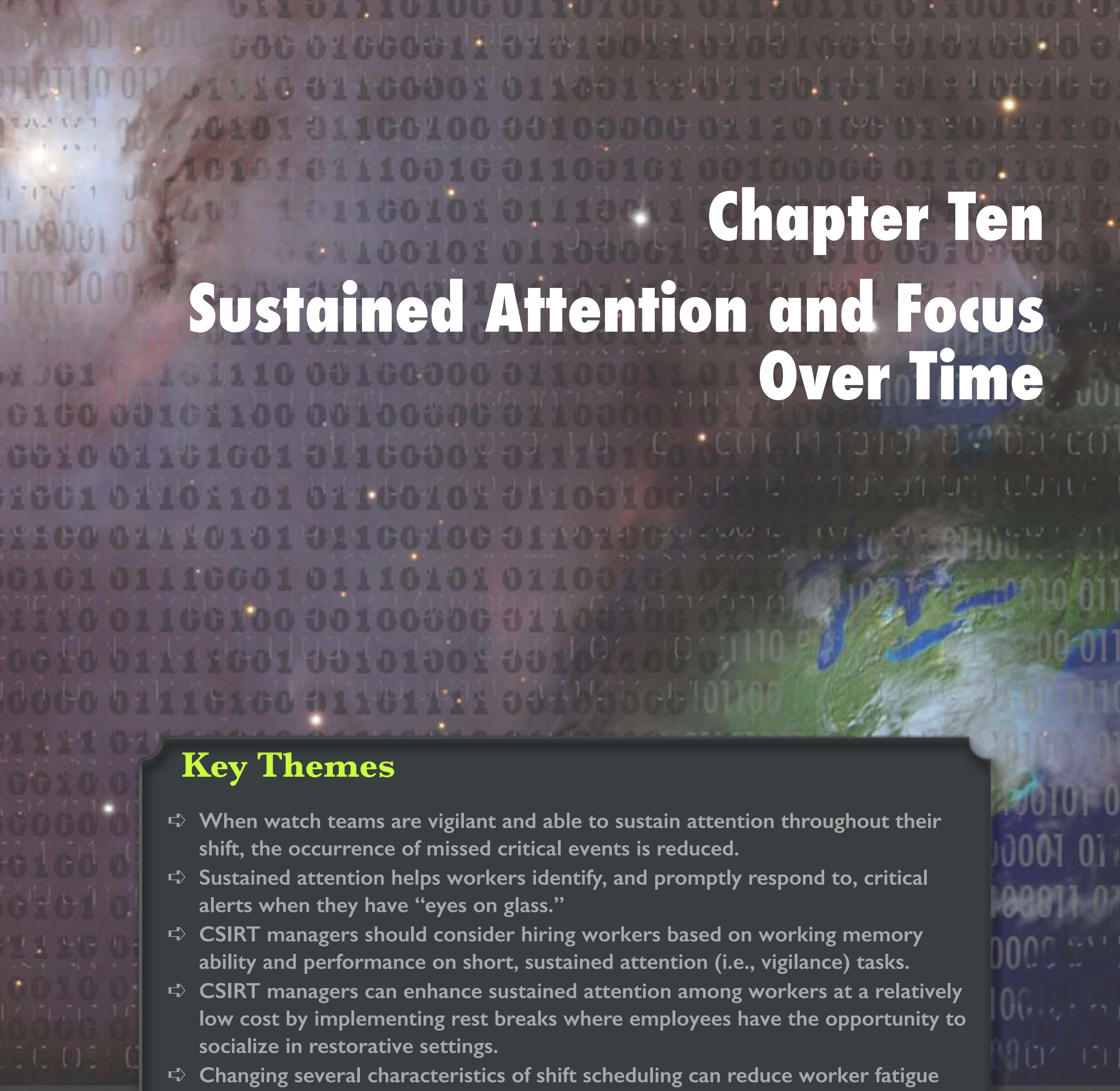
Tröster, C., & van Knippenberg, D. (2012). Leader openness, nationality dissimilarity, and voice in multinational management teams. *Journal of International Business Studies, 43*, 591-613.

Tyler, T. R., & Lind, E. A. (1992). A relational model of authority in groups. In M. Zanna (Ed.), *Advances in experimental social psychology* (Vol. 25, pp. 115-192). New York: Academic Press.

Ybarra, C. E., & Turk, T. A. (2009). The evolution of trust in information technology alliances. *The Journal of High Technology Management Research, 20*, 62-74.

Zaccaro, S. J., Weis, E. J., Hilton, R., & Jeffries, J. (2011). Building resilient teams. In P. J. Sweeney, M. D. Matthews, & P. B. Lester (Eds.), *Leadership in dangerous contexts: A handbook for the armed forces, emergency services, and first responders* (pp. 182-201). Naval Institute Press.

Zakaria, N., & Yusof, S. A. M. (2015). Can we count on you at a distance? The impact of culture on formation of swift trust within global virtual teams. In J. L. Wildman & G. Richard (Eds.), *Leading Global Teams: Translating Multidisciplinary Science to Practice* (pp. 253-268). Springer: New York.



Chapter Ten

Sustained Attention and Focus Over Time

Key Themes

- When watch teams are vigilant and able to sustain attention throughout their shift, the occurrence of missed critical events is reduced.
- Sustained attention helps workers identify, and promptly respond to, critical alerts when they have "eyes on glass."
- CSIRT managers should consider hiring workers based on working memory ability and performance on short, sustained attention (i.e., vigilance) tasks.
- CSIRT managers can enhance sustained attention among workers at a relatively low cost by implementing rest breaks where employees have the opportunity to socialize in restorative settings.
- Changing several characteristics of shift scheduling can reduce worker fatigue and, therefore, improve sustained attention, particularly for 24/7 operations that aim to maximize the attention of workers at all times of the day.

> “ ***Securitas Vigilantiae Instantis Praemium***
> *(British intelligence agency MI5's unorthodox Latin motto, intended to mean 'Security is the reward of unceasing vigilance').* ”
>
> ~ Andrew (2009)

Contents

10.0 Introduction

To identify and successfully respond to threats during a shift, CSIRT analysts must sustain attention and maintain focus. Social science researchers call this state of readiness "vigilance." Vigilance requires cognitive effort, and the continuous exertion of effort makes it difficult to maintain a high level of sustained attention over time (e.g., over the course of a long shift; Warm, Parasuraman, & Matthews, 2008). This chapter of the Handbook presents strategies to maximize performance and minimize decreases in attention over time.

> "I guess we kind of do what our manager calls 'eyes on glass'… we're looking through our clients, just making sure there's nothing going on and nothing looking suspicious."
>
> ~ CSIRT member

10.1 Assessing CSIRT Capacity for Sustained Attention

The following assessment exercise is designed to provide managers with a diagnostic tool in order to determine how well the CSIRT, individuals, or component teams within the CSIRT multiteam system (MTS) sustain attention. Based on the responses to this exercise, managers can determine whether they would benefit from the strategies offered in this chapter. Managers should consider the time and resources required to implement these strategies relative to their need for improvement.

Assess how your CSIRT is functioning in this area by responding to the following assessment on a 1-5 scale, where 1= Strongly Disagree, 2= Disagree, 3= Neither Agree nor Disagree, 4= Agree, 5= Strongly Agree.

GO TO PAGE 164 FOR
STRATEGIES FOR CSIRT MANAGERS

10.2 Background

10.2.1 THE IMPORTANCE OF SUSTAINED ATTENTION DURING INCIDENT RESPONSE

It is crucial that cybersecurity professionals are alert and recognize high-severity incidents in an ever-changing and dynamic environment. At any given time, some analysts focus on triaging thousands of incoming events into appropriate categories (e.g., new incidents, vulnerabilities, information requests, false positives)--a role informally referred to as "eyes on glass" or "the grind." Sustained attention is necessary in such tasks when: (a) the probability of critical incidents occurring is low, (b) the timing of these incidents is uncertain, and (c) prolonged periods of performance are necessary (e.g., when distinguishing critical incidents from the high volume of non-threatening incidents). CSIRTs, specifically monitoring or watch teams, engage in tasks that require sustained attention (e.g., Sawyer et al., 2014). Researchers who study sustained attention (i.e., vigilance) suggest strategies to enhance this focus over time. Sustained attention improves analyst performance and, hence, CSIRT performance. In this handbook section, we evaluate these strategies in terms of their relevance to CSIRTs and their cost effectiveness.

Although computer software (e.g., Security Information and Event Management, or SIEM, technology) can filter incidents so that more critical alerts are apparent, these programs are fallible and therefore require human oversight. The systems should alert the analyst whenever a serious incident (e.g., advanced persistent threat) is detected, so as to ensure that the analyst does not miss it; but, the criteria for an incident to pass through a mechanical filter must be low (e.g., the filter must risk false positives) and employees must analyze remaining incidents to determine whether they are critical. Analysts cannot ignore the system alerts because although some of the alerts may be false positives, other system alerts are for serious incidents. Sustained attention will help analysts detect critical incidents within the potentially high volume of system alerts.

ASSESSMENT EXERCISE	
1.	My employees pick up on critical incidents toward the ends of their shifts.
2.	My employees sustain their attention over the course of their shifts.
3.	My employees express satisfaction with the current scheduling of shifts and the length of shifts.
4.	My employees claim that shift scheduling leads to improvement in sustaining attention during their shifts.
5.	My employees appear to be alert at the end of their shifts.
6.	My employees remain focused when dealing with incidents that require overtime work or an extra shift.
7.	My employees take the correct amount of breaks during their shifts.
8.	After-action reviews have revealed success attributable to sustained attention on the part of an analyst.

When monitoring for incidents, two types of errors can occur: a false positive (e.g., reporting an incident as a threat when it really is not) or a false negative (e.g., not reporting an incident that really is a threat; Wickens, Hollands, Banbury, & Parasuraman, 2013). CSIRTs need to achieve an appropriate balance between false negatives and false positives. For high impact incidents, false negatives could be detrimental to the organization. Conversely, for low impact events, it might be desirable to reduce false positives, even at the expense of incurring false negatives. This chapter is primarily focused on low frequency, high severity incidents.

To detect genuine threats, a steady level of sustained attention among cybersecurity professionals is required; however, scanning a large number of events for critical incidents is cognitively demanding and requires constant attention. Attention depletes after continuous monitoring over the course of a shift and leads to less sensitivity in detecting critical incidents (Parasuraman, 1979), meaning that CSIRT members are less likely to find incidents over time-- especially if incidents are difficult to detect or differentiate from non-incidents. Decreased attention and less sensitivity increases response time and the number of missed incidents. For example, declines in critical incident detection over time occurred during a simulated cyber security task (Sawyer et al., 2014), where 13.8% more critical incidents were missed after 40 minutes on the task compared to after only 10 minutes on the task. Recent research indicates decreases in sustained attention can result in an increase in errors committed per minute accompanied by 45.1% more inconsistency in reaction times, which was associated with lower accuracy (Rosenberg, Noonan, DeGutis, & Esterman, 2013).

> **“The triaging is actually the prioritization. So how many resources do I want and need to spend for this issue? So usually there's a lot of things ongoing and you need to focus on the most important things.”**
>
> **~ CSIRT member**

10.2.2 SUSTAINED ATTENTION IN RELEVANT PROFESSIONS

Sustained attention is an important aspect in many other domains as well, and knowledge from those domains can benefit CSIRT work. Nursing is certainly one of these domains due to the serious consequences of errors on the job. A study of over 500 nurses discovered that longer shifts, common in nursing, were associated with decreased attention and increased risk of errors. Specifically, the risk of error (e.g., medication administration, procedural, charting, or transcription errors) nearly doubled, and nurses reported struggling to stay alert, when shifts exceeded 12.5 hours (Scott, Rogers, Hwang, & Zhang, 2006).

Sustained attention also is highly relevant for air traffic controllers. Air traffic controllers are responsible for monitoring large numbers of aircraft (“signals”) that simultaneously appear on radar. Separating signals from “noise” (i.e., non-aircraft) is difficult and can deplete attention (Langan-Fox, Sankey, & Canty, 2009). Results could be tragic if an air traffic controller misses a problem in their reduced state of attention and two planes cross paths. An FAA report on air traffic controllers found that almost two out of ten controllers committed an error, such as bringing planes close together, in the previous year (Orasanu et al., 2012). The report further mentioned that half of these controllers attributed their error to fatigue.

Even judicial rulings and the legal system are not immune to fatigue, as evidenced by the frightening findings of Danziger, Levav, and Avnaim-Pesso (2011), who found that judges’ favorable rulings gradually dropped from approximately 65% to nearly zero percent over the time period before a break. However, following a mid-day break, judges’ favorable rulings almost immediately returned to the 65% mark. These findings suggest that even judicial decisions, which should be based solely on facts, are susceptible to the devastating effects of fatigue. Sustained attention also is required in jobs such as X-ray baggage screening, quality control, and security video surveillance (Warm & Dember, 1998), that demonstrate similar attentional demands required of CSIRTs.

10.3 Project Findings

10.3.1 CSIRT POSITIONS THAT REQUIRE SUSTAINED ATTENTION

We interviewed 28 CSIRT multiteam systems (CSIRT MTSs) and *each one* reported having a team that clearly required sustained attention and focus over time to complete their tasks, such as a “Watch" team, “Monitoring and Response” team, or “Front/Triage" team. These teams monitor incoming incident traffic, queue incidents, determine priority, and determine whether incidents need to be handled or escalated to another team--all tasks that require attention over the entire course of a shift.

From our interviews with cybersecurity professionals, including their responses to surveys, we found that many CSIRT members think qualities and attributes related to sustained attention are important for effective performance in cybersecurity analyst positions. Below, we provide specific attributes related to sustained attention and the importance ratings from CSIRT members' surveys and/or CSIRT interviews.

10.3.2 KNOWLEDGE, SKILLS, ABILITIES, AND OTHER ATTRIBUTES (KSAOs) RELEVANT TO SUSTAINED ATTENTION

The following KSAOs were specifically mentioned in our interviews as important attributes for CSIRT employees (the percentage of CSIRTs that mentioned these KSAOs in their interviews is provided in parentheses):

- Attention to details (46.2%)

- Willingness to work shifts or be on call, which may include weekends or non-standard work hours (23.1%).

We also administered a separate survey to CSIRT members and asked them to rank the importance of various KSAOs. The characteristics relevant to sustained attention during incident response are provided below (percentages based on 85 survey respondents):

- 71.8% of respondents identified "Willingness to work shifts or be on call, which may include weekends or non-standard work hours" as important.
- 98.8% of respondents identified "Willingness to fully engage in tasks and diligence to complete them" as important.

10.3.3 COGNITIVE ABILITIES RELEVANT TO SUSTAINED ATTENTION

This project included cognitive task analyses to determine necessary cognitive abilities for CSIRT members to complete their tasks (see Appendix G for details). Interviewers asked CSIRT members to explain how they made decisions during past experiences. We identified the following cognitive abilities related to sustained attention (percentages based on 28 CSIRT CTA interviewees):

- 96% reported that Problem Sensitivity was important for identifying and mitigating a cybersecurity incident. Problem sensitivity is "the ability to tell when something is wrong or likely to go wrong" (Fleishman , Costanza, & Marshall-Mies, p. 179), and "it includes the specification of the problem as whole as well as recognition of the elements of the problem" (Fleishman , Quantaince, & Broedling, 2008, p. 322). Sustained attention and maintained focus are necessary to identify potential issues or vulnerabilities.
- 46% reported that Selective Attention was important for CSIRT effectiveness. "Selective attention is the ability to concentrate and not be distracted while performing a task over a period of time." (Fleishman , Costanza, & Marshall-Mies, 2008, p. 180).

These findings substantiate that CSIRT members believe sustained attention plays a strong role in CSIRT effectiveness. In the next section, we offer assessment questions CSIRT managers can use to evaluate the sustained attention of their team members, and later, present strategies to increase sustained attention among those team members.

10.4 Improving Sustained Attention and Focus over Time

Strategies designed to develop sustained attention and focus among CSIRT team members over time are provided in the next section. We recommend managers combine strategies that meet the specific needs of their team. Note that although sustained attention may be most important for the CSIRT's watch team, any team member engaged in cognitively taxing work arguably needs to be able to sustain attention over time. Thus, though this chapter focuses primarily on watch team members, these recommendations would also be relevant to members on other teams.

The goal of the following strategies is twofold: 1) ensure that eam members enter work shifts with the highest level of attention possible, and 2) ensure that eam members sustain and restore attention throughout work shifts. We will discuss hiring strategies to maximize attention capacity, as well as present shift design advice to ensure each individual arrives at work less fatigued and ready to provide maximum attention to his or her work. Shift design, in addition to rest breaks and time away from one's desk, should help sustain attention over the length of a shift.

There is not (yet) much good research on how to successfully train sustained attention. The research that does exist suggests that these training programs do not yield large improvements in sustained attention and would take a long time to execute, resulting in high costs and diversion of responsibilities on the job. At this point we do not recommend these training programs. Instead, we focus on hiring team members who already possess a high capacity for sustained attention. We also focus on more macro-level recommendations (e.g., work shift structure) that help to maximize team members' capacity for sustained attention. Managers can use the following strategies to maximize team members' attention capacity during cognitively demanding and tiring tasks.

10.4.1 STRATEGY 1: HIRE JOB APPLICANTS WHO DISPLAY A CAPACITY FOR SUSTAINED ATTENTION

One way to maximize team member attentiveness is to hire individuals who are better able to sustain attention and focus throughout their shifts. Selecting team members with higher levels of attention could be particularly beneficial for those teams whose tasks predominantly include surveillance tasks, such as monitoring and watch teams.

It is difficult to predict individual differences in sustained attention using measures of personality or intelligence. Instead, we suggest managers use an employee selection test including measures that predict sustained attention (Matthews, Warm, Shaw, & Finomore, 2010; Shaw, Matthews, Warm, Finomore, Silverman, & Costa, 2010).

Recommendations for use:

Two measures that would be particularly predictive of team members' sustained attention throughout their work shifts are a working memory task and a brief sustained attention (i.e., vigilance) task. It is recommended that organizations screen potential hires for each of those two qualities:

Working Memory Task

Working memory is the portion of memory that allows temporary storage of verbal or visual information. Temporary storage of information enables team members to sustain attention to perform their tasks. For instance, one study found a 95% likelihood (as opposed to the chance level of 50%) that people with better working memory would outperform people with worse working memory, in terms of sustained attention (Rose, Rendell, McDaniel, Aberle, & Kliegel, 2010). People differ in their working memory capacity, and these differences can be measured through a complex span task. A complex span task requires participants to keep information in their short-term memory while performing an additional task, known as a distraction task. Measuring working memory in a complex span task would not only identify participants' ability to keep information in their short-term memory, but also their ability to simultaneously complete the distraction task (Wickens & McCarley, 2008), which could be important when selecting employees who can maintain focus and attention in a complex environment.

A complex working memory span task can be created in several ways. In a reading memory span task, participants can read a series of sentences, verify whether each sentence makes sense (the distraction task), and then recall the last word of each sentence (the short term memory task). This task also can involve mathematical problems, where participants verify whether specific mathematical equations are correct (e.g., Does 1+1 = 2?). After a varying number of math equations are presented, participants are asked to recall digits that were listed to the right of the equal sign (Turner & Engle, 1989).

The task also can include a combination of numbers and words. In the operation-word-span or OSPAN task, participants alternate between verifying math problems and reading a word. After a series of problems and words, they are asked to recall the words. To measure one's operation span, the number of operation-word strings in a sequence will vary. A computerized example of this task can be found using the CogLab, the Online Cognition Lab website: https://coglab.cengage.com/labs/operation_span.shtml

Brief Vigilance (i.e., Sustained Attention) Tasks

Performance on a brief vigilance task can predict team members' performance on longer, sustained attention tasks, such as the monitoring task involved in incident response. One study demonstrated this phenomenon in a military context when researchers found that performance on a 12-minute activity involving monitoring pairs of letters in order to detect a critical signal (e.g., the letter combination of "OO") was positively related to performance on a one-hour vigilance task that involved scanning and detecting firing threats from military tanks (Matthews et al., 2010). Brief vigilance performance scores explained 21% to 28% of participants' ability to successfully monitor threats from military tanks in these scenarios (Matthews et al., 2010). This test could be revised for, and validated in (See Appendix C for validation guidelines), a CSIRT setting. For instance, in the CSIRT-specific version, the tanks could be replaced with cybersecurity-specific threats (e.g., a new critical incident).

Individual differences related to sustained attention can inform staffing decisions that result in improved employee performance and lower reduction of attention over time (e.g., over the course of a shift). Selecting new hires based on certain attributes (e.g., working memory) can streamline the hiring process and allow managers to hire employees who will succeed in the CSIRT environment, which requires constant attention and focus.

10.4.2 STRATEGY 2: ENCOURAGE EMPLOYEES TO INCORPORATE REST BREAKS INTO THEIR SHIFTS

Our interactions with CSIRT members pointed to the importance of periodic rest breaks during the workday. For instance, cybersecurity professionals in Sweden endorsed work "fika," which refers to taking a break, most often a coffee break. One large CSIRT we interviewed indicated they had no specific policy on breaks, which were taken at the discretion of employees. We propose that organizations or managers should provide suggestions to employees about how to incorporate rest breaks into their schedules and encourage employees to take more consistent and regular rest breaks.

Rest breaks help employees replenish attention that can help them maintain higher levels of performance throughout shifts. In a study on data entry workers, those workers who took two 15-minute breaks and four five-minute breaks during the work day, compared to those workers who only took two 15-minute breaks, had an increase of 3.27% in keystrokes per hour, despite taking 20 minutes more in breaks (Galinsky et al., 2007). Frequent rest breaks can also restore attention that will help team members maintain higher levels of performance (e.g., detecting critical incidents) throughout their shifts.

Rest breaks are important to maintain attention and focus and decrease fatigue. Additionally, rest breaks can incorporate aspects of relaxation and socialization that also positively impact attention.

Recommendations for use:

To effectively schedule rest pauses and breaks to minimize fatigue and maximize attentiveness, CSIRT managers should stress the importance of frequent, short rest breaks to team members. Specifically, managers should encourage team members to take approximately one 15-minute break every two hours (Boucsein & Thum, 1997; Tucker & Folkard, 2012). Of course, there will be instances where the suggested break time falls during a critical event that needs to be addressed. In these cases, managers should suggest that team members take their rest break after attending to the incident. An example schedule for an analyst could resemble the example in Table 10.1:

Managers also should allow team members some latitude regarding when to take breaks, rather than forcing adherence to a rigid break schedule. A rigid break schedule can result in

TABLE 10.1 SAMPLE SHIFT SCHEDULE, INCLUDING BREAKS, FOR AN ANALYST

SHIFT ACTIVITY	SHIFT TIME
Work	8:30 am – 10:30 am
Rest break	10:30 am – 10:45 am
Work	10:45 am – 12:45 pm
Lunch break	12:45 pm – 1:45 pm
Work	1:45 pm – 3:45 pm
Rest break	3:45 pm – 4:00 pm
Work	4:00 pm – 5:30 pm

Note: Different analysts would take breaks at slightly different times so as to ensure continuous "eyes on glass."

increased emotional strain for employees, possibly stemming from employees being interrupted in the middle of a complex task or train of thought (Boucsein & Thum, 1997). Providing a range of times in which a break should occur can help implement this suggestion. In addition to suggesting that team members take a break every two hours, managers can set a maximum amount of time before a team member must take a break, such as two and a half or three hours of work.

It is important to note that these breaks should be actual rest breaks that allow team members to disengage, as opposed to switching among different tasks, which does not restore attention (Ross, Russell, & Helton, 2014). An example of a rest break that could help replenish attention is to allow team members to adopt periodic "changes of scenery" during the workday (e.g., eating lunch away from their desk or utilizing their break to take a walk outdoors; Kaplan & Berman, 2010). Encouraging team members to incorporate rest breaks into their workday can help team members maintain focus during their shift. To restore attention, rest breaks should include restorative settings and socialization.

> **"[When discussing feeling tired or fatigued while at work] Interviewer: "What do you do to wake up?**
>
> **CSIRT Member: We all kind of get into our own, like own little zone…and we just kind of almost isolate ourselves…. but after a little while…we end up having a discussion…sometimes there's just that little interaction that just kind of gets your brain working on something else, that kind of snaps you out of it."**
>
> **~ CSIRT member**

Restorative Settings

Natural settings have been found to contribute to the replenishment of attention, necessary for sustained attention (Kaplan, 1995). Researchers found that reaction time decreased and attention on attentional task increased when participants were exposed to pictures of nature versus pictures of urban scenes (Berman, Jonides, & Kaplan, 2008). For instance, viewing greenery for merely 40 seconds during a break reduced errors Hartig, Mang, & Evans, 1991). Seemingly simple changes like incorporating pictures of natural, peaceful scenes in offices (Tang & Posner, 2009) or providing a quiet break room that overlooks green space or includes plants (Kaplan, 2001) can positively affect attention. The cost to implement some form of restorative setting in offices (e.g., plants, pictures of nature, break rooms with outdoor components or windows) is minimal.

Socialization

Informal interactions between employees can be a source of stimulation and variety in the work environment (Guest, Williams, & Dewe, 1978), reducing job monotony and boredom while positively influencing sustained attention (Dur & Sol, 2008; Morgeson & Humphrey, 2006). Managers should promote within-company informal social interactions during rest breaks. To effectively promote socialization, managers should:

1. Encourage employees to utilize a designated break room during their breaks where they can interact with other employees.
2. Urge newer employees to discuss, brainstorm, and problem-solve situations with more senior team members during work breaks.
3. Suggest team-building activities or tasks like "Free Fridays" at the company cafeteria, thereby encouraging employees to be more social while eating at the cafeteria with colleagues instead of at their desks alone.

Incorporating opportunities for socialization into rest breaks can provide employees with additional social benefits such as social support. Informal conversations between CSIRT members also encourage knowledge-sharing (see Chapter 8, "Shared Knowledge of Unique Expertise") and increase job satisfaction.

10.4.3 STRATEGY 3: SHIFT DESIGN – CREATE A SHIFT PLAN THAT REDUCES SLEEP DISTURBANCES AND MAXIMIZES ATTENTIVENESS

Our interviews with cybersecurity professionals demonstrated that shift lengths (e.g., 8-hour vs. 12-hour shifts) and shift rotations (e.g., morning→ afternoon → night → morning vs. morning→ night → afternoon → morning) differ across CSIRTs. Shifts can be implemented in a way that minimizes sleep disturbances and fatigue among employees by considering several shift characteristics described below.

Sleep and fatigue influence sustained attention. Decreases in the length of sleep or the quality of sleep can be detrimental to attention, resulting in more errors and slower reaction times. Researchers found that individuals who chronically sleep less (e.g., 4-6 hours of sleep) for two weeks demonstrate a 25% decrease in task performance on tasks that require sustained attention compared to those who sleep 8 hours (Van Dongen, Maislin, Mullington, & Dinges, 2003). In an extreme case scenario, pilots who experienced 24 hours of continued wakefulness demonstrated 20% slower reaction time and a 100% increase in incorrect responses to warnings during simulated flight activity (Caldwell, 2012). Thus, shift characteristics that minimize fatigue will enhance sustained attention. Sustained attention in turn will improve analyst performance (e.g., increase the likelihood an employee correctly identifies an incident as severe, even at the end of his or her shift)--and therefore team performance. We present several ways to optimize work shift characteristics with a focus on improved sustained attention.

Work Shift Characteristics

Shift Length (Eight-Hour Shifts Recommended)

Shift length is the amount of time employees work each time they come into the office. To improve sustained attention, managers should try to schedule team members for eight-hour work shifts as opposed to 12-hour shifts. Longer shifts are associated with more fatigue, as demonstrated by one study where poor sleep was reported 50% more two years after workers changed from eight-hour to 12-hour shifts (Yamada et al., 2001). As previously mentioned, poor sleep, or less hours of sleep, can relate to decreases in attention over time. For example, previous research has shown that, in the medical field, the risk of error doubled when shifts were longer than 12.5 hours. More nurses reported struggling to stay alert when they worked 8.5 to 12.5 hour shifts, compared to when they worked shifts shorter than 8.5 hours (Scott et al., 2006).

Some studies suggest that workers may prefer 12-hour shifts to increase time for social and leisure activities; however, there is limited support for this argument, and other studies have shown workers prefer eight-hour shifts (Ferguson & Dawson, 2012). Workers' preferences for eight-hour versus 12-hour shifts may vary based on individual circumstances (e.g., non-work factors such as family life). Because our focus is to schedule shifts that reduce fatigue and improve sustained attention, we suggest that team members be scheduled for eight-hour as opposed to 12-hour shifts.

Shift Rotation Speed (Rapid Shift Rotations Preferred)

Shift rotation implies that shifts change based on a set schedule. Shift rotation speed refers to the number of consecutive work shifts (i.e., number of consecutive times coming to work) until employees' shifts change (e.g., the start and end time of the shift changes). Managers should use rapid shift rotations (e.g., change shifts every week or couple of days rather than after several weeks) to increase team member alertness and reduce fatigue. Sleep loss accumulates as a function of the number of nights without sufficient sleep, suggesting that employees could more easily recover from two consecutive night shifts than from four consecutive night shifts (Härmä et al., 2006). Night shifts result in sleepiness because it is difficult to adjust to night activity due to circadian sleep patterns and light exposure (Åkerstedt, 2003).

A rapid shift rotation would have fewer consecutive night shifts than a slow shift rotation, which would reduce sleep loss that presumably builds after sleeping less each night shift and allow faster recovery from fatigue. One study compared rapid shift rotations consisting of 3 or 4 night shifts in a row to slow shift rotations with 7 consecutive night shifts, and the authors found that sleep quality was approximately 20% higher for employees on the rapid shift rotation compared to the slow shift rotation (Fischer et al., 1997).

Although circadian rhythms do not adjust by more than an hour a day (Folkard, Minors, & Waterhouse, 1991), we posit that if team members remain on the same shift for an extended period of time (e.g., two weeks), they might adjust to that sleep schedule. For instance, nurses who were permanent night workers had only slightly fewer correct reactions on an attention test at the beginning of their shifts (4.8% less) than nurses who worked night shifts on a rapidly rotating schedule (Petru, Wittmann, Nowak, Birkholz, & Angerer, 2005). Thus, using very slow shift rotations (i.e., change shifts every few weeks or more) could also reduce sleep disruptions (i.e., disturbances to circadian sleep rhythms; Monk & Folkard, 1992). However, rapidly rotating shifts are still considered more beneficial for several reasons, including less fatigue and more time for social contact.

A review of studies about permanent night shifts found the majority of employees (more than 97% of permanent night workers studied) never fully adjusted their natural sleep cycles (i.e., circadian rhythms) to night work (Folkard, 2008). These results imply that fatigue and sustained attention problems associated with night shifts might not be minimized among permanent night workers. Compared to a "fixed" night-shift, with a rapidly rotating shift schedule, team members can have more leisure time when family and friends are also available. With rapidly rotating shifts, team members can have evenings free every week (with evenings being the best time for social contact with friends and family), compared to a weekly rotating schedule, where social contact would be impossible during the two weeks they work evenings, and nights (Knauth, 1996), or compared to a permanent night shift, where social contact would always be impossible on nights they are working.

Shift Rotation Direction (Forward Shift Rotation Preferred)

Shifts typically rotate in a forward or backward direction. When possible, managers should use forward shift rotations (i.e., morning→afternoon → night→morning) rather than backward shift rotations (i.e., morning → night → afternoon→morning). Research indicates that people acclimate more easily to time zone changes that move clockwise, or westward (Dement & Vaughan, 1999; Tucker & Folkard, 2012). Similarly, shift rotations should move clockwise, or forward, to avoid major disruptions to team members' circadian rhythm and to improve sleep quality. One study found that, compared to shift workers on a forward shift rotation, more shift workers on a backwards shift rotation experienced poor sleep quality (van Amelsvoort, Jansen, Swaen, van den Brandt, & Kant, 2004).

Effectiveness Evidence:

It is important to evaluate the costs associated with shift design changes. Although shift characteristics improve the alertness and attentiveness of CSIRT members, managers should be aware of the potential costs these changes will simultaneously involve. Changing existing longer shift lengths (e.g., 12 hours) to eight hours will require a small amount of additional staff time to arrange shift logistics and, more importantly, could increase staffing costs (i.e., more team members might be needed). Changing shift rotation speed from slow to fast also will include costs to arrange logistics. Changing shift direction (i.e., from backwards to forwards rotation) might not require as many costs, assuming that the shifts are already scheduled in a rotating fashion.

If managers change shift characteristics, consideration should be given to "handoffs" of important information from one team member to the next. For instance, using eight-hour shifts, as opposed to 12-hour shifts, means more handoffs of job tasks will occur throughout each day (e.g., between the morning, mid-day, and night shifts). To make handoffs as efficient as possible, steps should be taken to ensure necessary information is transferred efficiently (see Chapter 5, "Communication Effectiveness in Incident Response," for more information). Such pertinent information can include event status and actions taken during similar previous events. To transfer this information, and reduce errors and miscommunications, managers should implement standardized formats for handoffs (Starmer et al., 2014). For instance, research in the medical field suggests that handoffs should be both oral and written (Cleland, Ross, Miller, & Patey, 2009). Written handoffs provide documentation so that information is not forgotten, and oral discussion during the handoffs ensures that incoming shift employees are updated and have the opportunity to ask questions or seek clarification.

Managers should anticipate potentially negative reactions from team members in the short run, as any shift change (i.e., shift length, shift rotation) will impact their existing work and personal schedules. Although some negative reactions may result from changes, reducing shift length and adopting a forward, rapidly rotating shift schedule can improve sleep quality and reduce fatigue. Ultimately, this will help team members sustain attention and focus throughout their shifts in order to better detect critical incidents.

10.5 Chapter Summary

Some cybersecurity professionals we interviewed reported that team members sometimes look for critical events over extended periods of time (e.g., "eyes on glass"). To improve sustained attention and focus over time, managers should implement as many of our recommended strategies as possible. However, some strategies might not be applicable to specific CSIRTs, or might be too costly to implement. For instance, if shift lengths, rotations, and length of breaks cannot be changed, managers could nonetheless provide suggestions for employees regarding the best use of rest breaks (e.g., incorporating socialization). Additionally, managers could select team members based upon their ability to sustain attention; however, managers first must validate employee selection tools to ensure that working memory and brief sustained attention (i.e., vigilance) tasks predict sustained attention in CSIRT team members.

Managers need to determine the primary factor influencing team members' performance, such as whether team members come to work tired or lose steam throughout work-shifts. Shift-length and shift-rotation decisions are useful strategies to address team member fatigue, whereas rest break strategies address decreases in attention over the length of a work-shift. All of these factors impact effective cybersecurity incident response, particularly during critical times that require sufficient attention and cognitive endurance.

References

Åkerstedt, T. (2003). Shift work and disturbed sleep/wakefulness. *Occupational Medicine*, 53(2), 89-94.

Andrew, C. (2009). *The defence of the realm: The authorized history of MI5*. London, UK: Allen Lane.

Berman, M. G., Jonides, J., & Kaplan, S. (2008). The cognitive benefits of interacting with nature. *Psychological Science, 19*, 1207-1212.

Boucsein, W. & Thum, M. (1997). Design of work/rest schedules for computer work based on psychophysiological recovery measures. *International Journal of Industrial Ergonomics, 20*, 51-57.

Caldwell, J.A. (2012). Crew schedules, sleep deprivation, and aviation performance. *Current Directions in Psychological Science, 21*(2), 85-89.

Cleland, J. A., Ross, S., Miller, S. C., & Patey, R. (2009). "There is a chain of Chinese whispers…": empirical data support the call to formally teach handover to prequalification doctors. *Quality and Safety in Health Care, 18*(4), 267-271.

Danziger, S., Levav, J., & Avnaim-Pesso, L. (2011). Extraneous factors in judicial decisions. *Proceedings of the National Academy of Sciences, 108* (17), 6889-6892.

Dement, W. C., & Vaughan, C. (1999). *The promise of sleep: A pioneer in sleep medicine explores the vital connection between health, happiness, and a good night's sleep*. New York: Delcorte.

Dur, R. & Sol, J. (2008). *Social interaction, altruism, and incentives at the workplace* (Paper No. 2476). CESIFO Working Paper.

Ferguson, S. & Dawson, D. (2012). 12-h or 8-h shifts? It depends. *Sleep Medicine Reviews,* 16, 519-528.

Fischer, F. M., Bruni, A. C., Berwerth, A., Moreno, C. R. C., Fernandez, R. L., & Riviello, C. (1997). Do weekly and fast-rotating shiftwork schedules differentially affect duration and quality of sleep? *International Archives of Occupational and Environmental Health, 69*(5), 354-360.

Fleishman, E. A., Costanza, D. P., & Marshall-Mies, J. (1999). Abilities. In N. G. Peterson, M. D. Mumford, W. C. Borman, P. R. Jeanneret, and E. A. Fleishman (Eds.), An occupational information system for the 21st Century: The development of O*NET. Washington DC: American Psychological Association.

Fleishman, E. A., Quaintance, M. K., & Broedling, L. A. (2008). Taxonomies of human performance. Bethesda, MD: Management Research Institute.

Folkard, S. (2008). Do permanent night workers show circadian adjustment? A review based on the endogenous melatonin rhythm. *Chronobiology international, 25*(2-3), 215-224.

Folkard, S., Minors, D. S., & Waterhouse, J. M. (1991). " Demasking" the temperature rhythm after simulated time zone transitions. *Journal of Biological Rhythms, 6*(1), 81-91.

Galinsky, T., Swanson, N., Sauter, S., Dunkin, R., Hurrell, J., & Schleifer, L. (2007). Supplementary breaks and stretching exercises for data entry operators: A follow-up field study. *American Journal of Industrial Medicine, 50*(7), 519-527.

Guest, D., Williams, R., & Dewe, P. (1978). Job design and the psychology of boredom. Paper presented at the 19th International Congress of Applied Psychology, Munich, West Germany.

Härmä, M., Tarja, H., Irja, K., Mikael, S., Jussi, V., Anne, B., & Pertti, M. (2006). A controlled intervention study on the effects of a very rapidly forward rotating shift system on sleep–wakefulness and well-being among young and elderly shift workers. *International Journal of Psychophysiology, 59*(1), 70-79.

Hartig, T., Mang, M., & Evans, G. W. (1991). Restorative effects of natural environment experiences. *Environment and Behavior, 23(1)*, 3-26.

Kaplan, R. (2001). The nature of the view from home: Psychological benefits. *Environment and Behavior, 33(4)*, 507-542.

Kaplan, S. (1995). The restorative benefits of nature: Toward an integrative framework. *Journal of Environmental Psychology, 15*, 169-182.

Kaplan, S. & Berman, M.G. (2010). Directed attention as a common resource for executive functioning and self-regulation. *Perspectives on Psychological Science, 5*(1), 43-57.

Knauth, P. (1996). Designing better shift systems. *Applied Ergonomics, 27*(1), 39-44.

Langan-Fox, J., Sankey, M.J., & Canty, J.M. (2009). Human factors measurement for future air traffic control systems. *Human Factors, 51*(5), 595-637.

Matthews, G., Warm, J. S., Shaw, T. H., & Finomore, V. S. (2010). A multivariate test battery for predicting vigilance. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 54* (14), 1072-1076. SAGE Publications.

Monk, T. H., & Folkard, S. (1992). *Making shift work tolerable*. London: Taylor & Francis.

Morgeson, F.P. & Humphrey, S.E. (2006). The Work Design Questionnaire (WDQ): Developing and validating a comprehensive measure for assessing job design and the nature of work. *Journal of Applied Psychology, 91*(6), 1321-1339.

Orasanu, J., Parke, B., Kraft, N., Tada, Y., Hobbs, A., Anderson, B., ... & Dulchinos, V. (2012). *Evaluating the effectiveness of schedule changes for air traffic service (ATS) providers: Controller alertness and fatigue monitoring study* (Report No. DOT/FAA/HFD-13/001). Washington, D.C.: Federal Aviation Administration.

Parasuraman, R. (1979). Memory load and event rate control sensitivity decrements in sustained attention. *Science, 205*(4409), 924-927.

Petru, R., Wittmann, M., Nowak, D., Birkholz, B., & Angerer, P. (2005). Effects of working permanent night shifts and two shifts on cognitive and psychomotor performance. International archives of occupational and environmental health, 78(2), 109-116.

Rose, N. S., Rendell, P. G., McDaniel, M. A., Aberle, I., & Kliegel, M. (2010). Age and individual differences in prospective memory during a" Virtual Week": The roles of working memory, vigilance, task regularity, and cue focality. *Psychology and Aging, 25*(3), 595-605.

Rosenberg, M., Noonan, S., DeGutis, J., & Esterman, M. (2013). Sustaining visual attention in the face of distraction: A novel gradual-onset continuous performance task. *Attention, Perception, & Psychophysics, 75*(3), 426-439.

Ross, H. A., Russell, P. N., & Helton, W. S. (2014). Effects of breaks and goal switches on the vigilance decrement. *Experimental Brain*

Research, 232(6), 1729-1737.

Sawyer, B. D., Finomore, V. S., Funke, G. J., Mancuso, V. F., Funke, M. E., Matthews, G., & Warm, J. S. (2014). Cyber vigilance effects of signal probability and event rate. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58*, 1771-1775.

Scott, L. D., Rogers, A. E., Hwang, W. T., & Zhang, Y. (2006). Effects of critical care nurses' work hours on vigilance and patients' safety. *American Journal of Critical Care, 15*(1), 30-37.

Shaw, T. H., Matthews, G., Warm, J. S., Finomore, V. S., Silverman, L., & Costa, P. T. (2010). Individual differences in vigilance: Personality, ability and states of stress. *Journal of Research in Personality, 44*(3), 297-308.

Starmer, A. J., Spector, N. D., Srivastava, R., West, D. C., Rosenbluth, G., Allen, A. D., … Landrigan, C. P. (2014). Changes in medical errors after implementation of a handoff program. *The New England Journal of Medicine, 371(19)*, 1803-1812.

Tang, Y. Y., & Posner, M. I. (2009). Attention training and attention state training. *Trends in Cognitive Sciences, 13(5)*, 222-227.

Tucker, P., & Folkard, S. (2012). *Working time, health and safety: A research synthesis paper.* ILO.

Turner, M. L., & Engle, R. W. (1989). Is working memory capacity task dependent? *Journal of Memory and Language, 28*, 127-154.

Van Amelsvoort, L. G., Jansen, N. W., Swaen, G. M., Van Den Brandt, P. A., & Kant, I. (2004). Direction of shift rotation among three-shift workers in relation to psychological health and work-family conflict. *Scandinavian Journal of Work, Environment & Health, 15*, 149-156.

Van Dongen, H. P., Maislin, G., Mullington, J. M., & Dinges, D. F. (2003). The cumulative cost of additional wakefulness: dose-response effects on neurobehavioral functions and sleep physiology from chronic sleep restriction and total sleep deprivation. *SLEEP, 26*(2), 117-129.

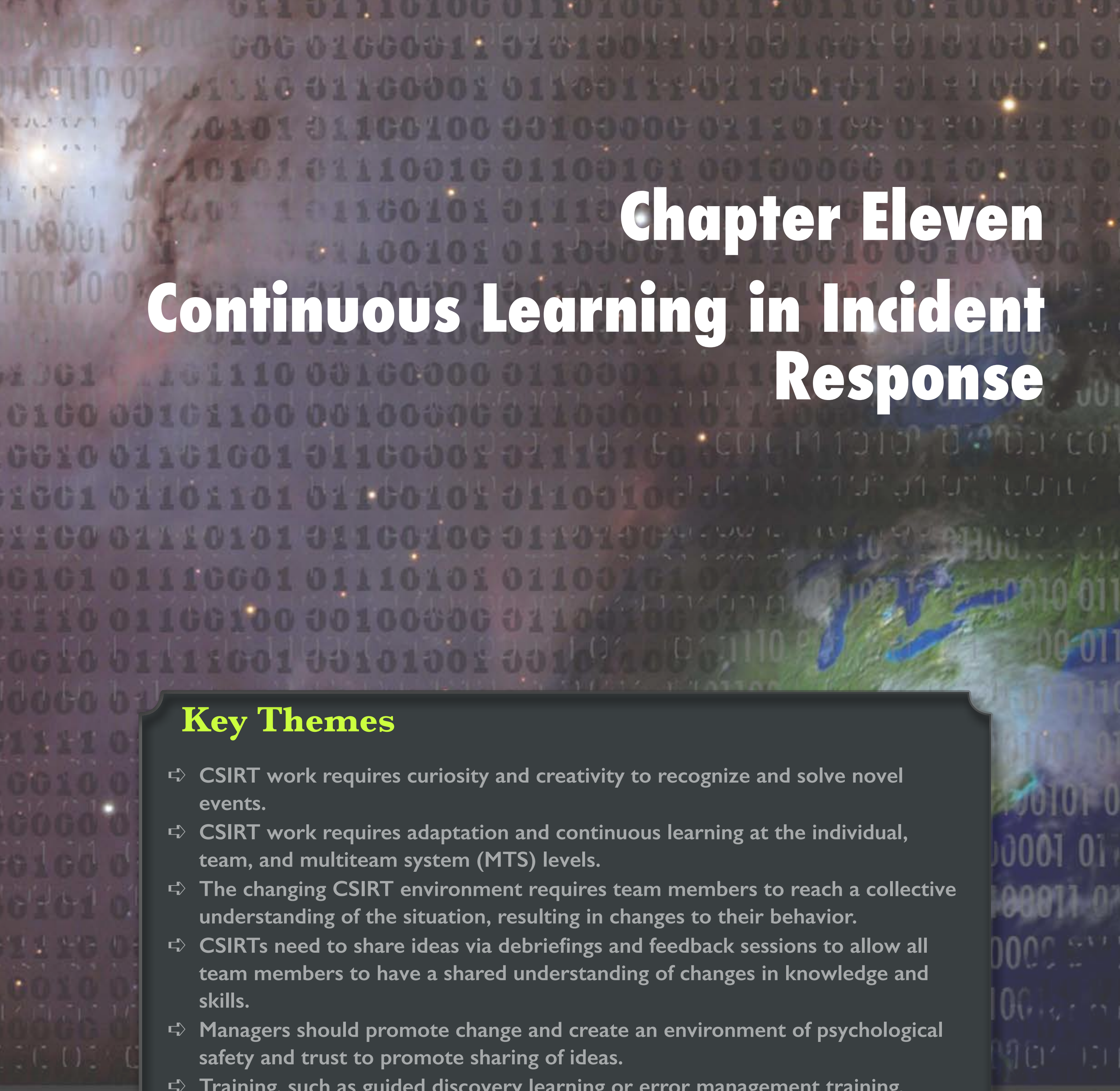
Warm, J.S. & Dember, W.N. (1998). Tests of vigilance taxonomy. In: R.R. Hoffman, M.F. Sherrick, and J.S. Warm (Eds.). *Viewing psychology as a whole: The integrative science of William N. Dember*. Washington, DC: American Psychological Association.

Warm, J. S., Parasuraman, R., & Matthews, G. (2008). Vigilance requires hard mental work and is stressful. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 50*(3), 433-441.

Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2013). *Engineering psychology and human performance* (4th Ed.). USA: Pearson Education, Inc.

Wickens, C. D., & McCarley, J. (2008). *Applied attention theory*. Boca Raton, FL: Taylor & Francis.

Yamada, Y., Kameda, M., Noborisaka, Y., Suzuki, H., Honda, M., & Yamada, S. (2001). Excessive fatigue and weight gain among cleanroom workers after changing from an 8-hour to a 12-hour shift. *Scandinavian Journal of Work, Environment & Health, 27*, 318-326.



Chapter Eleven

Continuous Learning in Incident Response

Key Themes

- CSIRT work requires curiosity and creativity to recognize and solve novel events.
- CSIRT work requires adaptation and continuous learning at the individual, team, and multiteam system (MTS) levels.
- The changing CSIRT environment requires team members to reach a collective understanding of the situation, resulting in changes to their behavior.
- CSIRTs need to share ideas via debriefings and feedback sessions to allow all team members to have a shared understanding of changes in knowledge and skills.
- Managers should promote change and create an environment of psychological safety and trust to promote sharing of ideas.
- Training, such as guided discovery learning or error management training, facilitates learning among team members, contributing to team learning processes.
- Learned knowledge must be stored, either in the memories of team members or in knowledge databases (e.g., wikis), and be retrievable when needed.

Contents

11.0 Introduction

Cybersecurity incident response work occurs in a dynamic environment. To keep up with developments in the field, cybersecurity analysts need to continuously learn new skills, and identify new and useful solutions to novel situations, in order to respond to threats to organizations' infrastructures (Chen et al., 2014). This chapter provides guidance for managers on how to create and maintain a climate for learning where individuals, CSIRTs, and organizations are supported for learning (Nikolova, Van Ruysseveldt, De Witte, & Van Dam, 2014). A learning climate includes policies, practices, and reward systems that facilitate learning and the generation and implementation of innovative ideas (Sung & Choi, 2014), provide employee advancement and development opportunities (Govaerts, Kyndt, Dochy, & Baert, 2011), and tolerate errors made during the learning process (Nikolova et al., 2014). Positive learning climates result in lower turnover intentions, less stress, and higher job satisfaction (Egan Yang, & Bartlett, 2004; Nikolova et al., 2014). Furthermore, employee performance is improved with new knowledge (Marsick & Watkins, 2003) and employees are more committed to the organization when their job offers learning opportunities (Armstrong-Stassen & Schlosser, 2008).

11.1 Assessing Continuous Learning

The following assessment exercise is designed to provide managers with a diagnostic tool in order to determine how well the CSIRT, individuals, or component teams within the CSIRT multiteam system (MTS) are engaging in continuous learning. This will ultimately help determine the social maturity of the CSIRT (See Chapter 2, "The Social Maturity of CSIRTs and Multiteam Systems," for additional information). The assessment is grouped by topics covered in this chapter. Based on the responses to this assessment, managers can determine whether they would benefit from the strategies offered in this chapter. Managers should consider the time and resources required to implement these strategies relative to the CSIRT's need for improvement.

Assess how your CSIRT is functioning in this area by responding to the following assessment on a 1-5 scale, where 1= Strongly Disagree, 2= Disagree, 3= Neither Agree nor Disagree, 4= Agree, 5= Strongly Agree.

ASSESSMENT EXERCISE – OVERALL CONTINUOUS LEARNING

INDIVIDUAL AND TEAM LEARNING

1. Team members keep up to date with developments in cybersecurity.
2. The design of cybersecurity personnel's work roles allows them to develop new skills.
3. Team members engage others outside of your organization to gain new knowledge and skills.
4. Team members maintain contacts with other cybersecurity professionals in order to learn new knowledge and skills.
5. Team members have the opportunity to try out new ideas and processes.

MULTITEAM SYSTEM LEARNING

1. Teams discuss how they should interact differently as a result of previous incidents (e.g., in after-action reviews).
2. Thinking about "lessons learned" regarding team interactions or after-action reviews occurs in a timely manner after events.
3. Multiple teams working together have the opportunity to try new ideas or processes.
4. Teams participate in activities where they can make errors and learn from their mistakes without these errors being detrimental to the CSIRT performance (e.g., during training exercises).
5. Multiteam information databases (e.g., a wiki, information board) are used in events.
6. Multiteam information databases (e.g., a wiki, information board) are used in training.

ASSESSMENT EXERCISE – INDIVIDUAL LEARNING RELATED TO CREATIVITY AND CURIOSITY

1. Team members exhibit an eagerness to learn.
2. Team members try to solve problems even when not presented with a specific problem or incident.
3. Team members seek new cybersecurity-related knowledge.
4. Team members keep searching for information until they are able to understand complex issues instead of giving up.

GO TO PAGE 178 FOR STRATEGIES FOR CSIRT MANAGERS TO PROMOTE LEARNING THROUGH CREATIVITY AND CURIOSITY

ASSESSMENT EXERCISE – ENHANCING LEARNING THROUGH WORK DESIGN

1. Work tasks required of your team members provide them with the opportunity to develop new skills.
2. Work roles of your team members allow them to influence their own work situation, working methods, and pace of work, enabling them to learn new skills.
3. Team members get timely feedback about their work, resulting in learning.

GO TO PAGE 180 FOR STRATEGIES FOR CSIRT MANAGERS TO PROMOTE LEARNING THROUGH WORK DESIGN

ASSESSMENT EXERCISE – DEVELOPMENTAL NETWORKS AND NETWORKING SKILLS

1. Team members proactively establish relationships with people inside your organization(s) in order to learn new knowledge and skills.
2. Team members proactively establish relationships with people outside your organization(s) in order to learn new knowledge and skills.
3. Team members network with others outside your team in order to learn new knowledge and skills.

GO TO PAGE 181 FOR STRATEGIES FOR CSIRT MANAGERS TO PROMOTE LEARNING THROUGH DEVELOPMENTAL NETWORKS AND ENCOURAGING NETWORKING BEHAVIORS

ASSESSMENT EXERCISE – TEAM LEARNING

SHARING

1. Team members discuss among themselves how they should change their behaviors as a result of previous incidents (e.g., in after-action reviews).
2. Thinking about "lessons learned," or after-action reviews occurs in a timely manner after events?
3. Team members network with others outside your team in order to learn new knowledge and skills.

EXPERIMENTING TO LEARN

1. Team members have the opportunity to try new ideas or processes.
2. Team members participate in activities where they can make errors and learn from their mistakes without these errors being detrimental to the CSIRT performance (e.g., during training exercises) or individual performance evaluations.

STORING/ RETRIEVING

1. Information databases (e.g., a wiki, information board) are used to learn about events.
2. Information databases (e.g., a wiki, information board) are used in training.

GO TO PAGE 182 FOR STRATEGIES FOR CSIRT MANAGERS TO PROMOTE TEAM LEARNING

11.2 Background

Cybersecurity work requires continuous learning among individual analysts, teams and MTSs. Certain individual characteristics of employees can facilitate continuous learning; however, the policies, practices and reward systems that are in place are necessary to sustain a learning climate. This section of the Handbook reviews relevant organizational science literature and the findings from our research project that are relevant to individual and team learning. Then, strategies and recommendations for maintaining continuous learning are presented.

11.2.1 CREATIVITY AND CURIOSITY

The dynamic nature of the cybersecurity work environment represents a challenge to analysts. They are frequently faced with novel, complex and ambiguous situations. To address these situations, analysts must engage in continuous learning, seeking new information to keep up with new developments in cybersecurity threats and technical solutions to these threats.

Creativity is the generation of new ideas that are useful (Amabile, 1988).. The literature on creativity training has found that training focused on generating ideas, finding specific problems, and combining different concepts to create novel solutions, was the most effective in improving creativity (Scott, Leritz & Mumford, 2004). To a certain extent, creativity must start at the individual level because idea generation or creation is an individual activity. The effectiveness of the creativity training techniques stems from providing people with strategies for working with what they already knew, which is consistent with the research literature that finds that creativity is based on individuals' background, knowledge, and experience (e.g., Mumford, Antes, Caughron, Connelly & Beeler, 2010).

Curiosity is "a desire for knowledge that motivates individuals to learn new ideas, eliminate information gaps, and solve intellectual problems" (As cited in Litman, 2008, p. 1596). CSIRT work, which involves complex problem-solving and critical decision-making, often occurs in highly ambiguous situations. These situations require individuals to mentally solve complicated problems related to unexpected incidents and to work through situations never before encountered. Individuals need to purposefully seek out novel situations and to explore situations, especially complex and ambiguous events or situations.

Creativity and curiosity are strongly related to each other and have been found to be related to a variety of important work outcomes. For example, curiosity has been found to strongly relate to job performance, with performance measured as a combination of task performance, attainment of supervisory assigned goals, and job knowledge and skills (Mussel, 2013). Curiosity also influences job performance for new employees by positively affecting their adoption of organizational values, goals, attitudes (Reio & Wiswell, 2000), and the way employees frame new situations, which, in turn,

> “The reason I believe that you don’t want to follow the exact same steps every time [is] because you have to leave room for creativity and interpretation. You can’t just go blind,…you have to leave a lot of room for improving and adapting and overcoming.”
>
> ~ CSIRT Member

influences job performance. Lastly, curiosity enhances information seeking, which, in turn, enhances job performance (Harrison, Sluss, & Ashforth, 2011).

Beyond job performance, curiosity is related to employees’ tendency to enjoy thinking (Cacioppo, Petty, & Kao, 1984) and to perform mentally challenging tasks (Ackerman, Kanfer & Goff, 1995, as reported by Mussel, 2010). In addition, curious people tend to focus on developing new skills and knowledge (Dweck, 1986; Mussel, 2011). Thus, individuals who are curious would fit well with the CSIRT environment, and the presence of a strong climate for learning would attract and retain cybersecurity personnel with high levels of curiosity and creativity. A strong learning climate matches CSIRTs’ main tasks, which rely heavily on dynamic information technology that requires the acquisition and application of knowledge (Sørensen & Holman, 2014).

> “…We’re looking for a hacker...[we’re] like an astronaut... the explorer nature. They want to see the unknown – will always try to fix a clock, even if it’s not broken.”
>
> ~ CSIRT Member

11.2.2 DEVELOPMENTAL NETWORKS AND NETWORKING BEHAVIOR

CSIRT members are embedded in a professional network of other CSIRT professionals. These individuals may be within their own CSIRT, but they may also be individuals in other similar organizations, client organizations, professional associations, or educational communities. Networks are important to the success of individuals, teams, and organizations (de Janasz & Forret, 2008; McCauley & Douglas, 2004). Networks can help CSIRT professionals in learning important knowledge and skills as well as accessing information. Characteristics of a network, such as who is in the network, how large the network is, where an individual is located in the network, and the strength of different connections between people in the network, can influence the amount of learning that takes place. It is often thought that the larger the network the better it is for learning. Conjar (2014), though, found that size may not be as important as previously thought and large networks can actually have negative effects—presumably because larger networks require more effort to maintain the relationships among the various individuals in the network. Conjar's study, however, also indicated that the diversity represented by network members’ disciplines, organizational functions, and background was key to learning and development.

> “…experience to understand how networks and communications and other systems interact with each other. I mean it’s solving a puzzle is what it is. So you have to have somebody that’s going to be naturally curious, I guess, and want to solve that puzzle.”
>
> ~ CSIRT Member

Networking includes "behaviors...aimed at building, maintaining, and using informal relationships that possess the (potential) benefit of facilitating work-related activities of individuals by voluntarily granting access to resources and maximizing common advantages" (Wolff & Moser, 2009, pp. 196–197; see also Forret & Dougherty, 2004; Oldham & Da Silva, 2015; Wolff & Moser, 2006). Previous research has found that the larger the network the more task-relevant and diverse information the network has (Anderson, 2008), and the more innovative the network is (McFadyen & Cannella, 2004), but this may have limits. For example, there is a tendency for people to be attracted to similar people if a conscious effort is not made to include people who have different backgrounds in the developmental network. In a scenario where that effort is not made, information diversity will be narrowed and the learning potential of the network is reduced (Conjar, 2014). To build a developmental network that facilitates learning, effort must be made to create a network that connects others with the necessary information and resources to facilitate learning.

> “Sometimes people know somebody within the organization. A very similar thing, sometimes you don’t know or you need to find the information about something. Oh, yeah, go to the directory or go to the social things…and ask.”
>
> ~ CSIRT Member

Developmental networks should be constructed in a way that includes people who can provide (a) a means of helping learners assess their strengths and learning needs, (b) advice on where to find challenging growth experiences, and (c) support to persist through such challenges (Conjar, 2014; McCauley & Douglas, 2004; Van Velsor & McCarthy, 2004). Developmental partners help motivate CSIRT members to master new skills (Van Velsor & McCauley, 2004), to persist when experiencing difficulties in the learning process (Ratwani, Zaccaro, Garven, & Geller, 2010), and to obtain necessary learning resources (Cross & Thomas, 2008).

> I do not believe in us trying to track all the individuals we need to talk to. I track the executives I need to talk to. They know their teams better than I know their teams, so they know the right people to pull in. And it also gives them the responsibility. So I know who our general counsel is, right, I know that individual. They know who all their people, so they'll pull those individuals in. So our process is tied directly to the role of the executive and the people we need to pull in.
>
> ~ CSIRT Member

11.2.3 TEAM LEARNING

CSIRTs grow and develop together to accomplish tasks. One way to evolve together is through team learning. Team learning is not merely individual team members learning. Rather, team learning occurs when the group comes to a collective understanding, likely through shared experiences. This change in the team's "team's collective...knowledge and skill" (i.e., team learning; Ellis, et al., 2003, p. 822) provides the team with a broader range of possible behaviors that could contribute to improved task performance (Wilson, Goodman, & Cronin, 2007). When the team learns, all team members experience a change in knowledge that can then result in a change in routines and behaviors (Wilson et al., 2007). The organization and environment of CSIRTs changes frequently, and incidents are constantly evolving and changing. Therefore, it is important that the team learns so that they can apply this knowledge to other incidents. Because teams are important for organizations to be effective, managers must create an environment, and put in place processes, to facilitate team learning.

Knowledge Sharing

For all group members to understand new knowledge, routines, and behaviors, the process of *sharing* must occur. Individuals acquire knowledge, but for the team as a whole to learn, team members must share what they know (Hofmann & Frese, 2011). There are three steps to sharing knowledge (Wilson et al., 2007):

1. An individual learns something new (e.g., knowledge, routine, behavior)
   - CSIRT Example: An individual has read of a new technique to mitigate an incident.
2. Group members gain the same understanding
   - CSIRT Example: The individual discusses this new technique with other team members so that all the team members understand this new technique.
3. Knowledge is transferred to new group members
   - CSIRT Example: New members of the team are informed of this new technique as part of their onboarding (e.g., training for new team members).

One way to reduce incomplete sharing is for the team to learn together and learn from each other. Teams can share knowledge by collectively reflecting on previous events, listening carefully to their teammates, and addressing differences in opinions (Van den Bossche, Gijselaers, Segers, & Kirschner, 2006). When teams come to a mutual agreement about new knowledge, behavior, or routines, they are more likely to use them in future events. In the strategies and recommendations in this chapter, ways to improve team reflection processes and, in turn, facilitate team learning are provided.

Team learning and reflection can also occur outside of the processes that take place following incidents or events occurring at work. For example, managers can encourage and facilitate team learning through training activities. These activities can facilitate the processes necessary for teams to learn in *real* work situations. In situations that are only for learning (e.g., not on-the-job training), mistakes may not be detrimental; therefore, the team can learn by trying new things and making errors along the way. These *discovery*, or *experimental*, learning exercises can help teams practice reflection and build shared understandings of new information. Error management training (see Recommendation 10 in this chapter) helps team members learn from their errors, but also helps build trust within the team. These activities help the team develop their reflection techniques and shared understandings that can be applied to learning in work situations.

> I like to have a spirit in the team where everybody is not only eager to get knowledge, but also eager to share knowledge.
>
> ~ CSIRT Member

Knowledge Storage and Retrieval

After teams develop a shared understanding, they need a way to store this inventory of new knowledge, behaviors, and routines for future use. Storing is important in team learning because knowledge learned by the group needs to be retained. There are two ways to store knowledge: one is to physically record the new knowledge, behaviors, or routines in a database or bulletin board, and the other is to store knowledge via group members' memories. Shared knowledge of unique expertise (SKUE) is an example of group memory storage where team members know their own expertise and the other team members' expertise (See Chapter 8, "Shared Knowledge of Unique Expertise"). With SKUE, team members know who is responsible for what type of information, making it clear (1) who needs to "store" specific learned information; and (2) who to ask to retrieve specific "stored" information. For instance, one team member may be good at developing software to detect events. That team member needs to know that he or she is responsible for any software-related knowledge. Additionally, the team needs to know to go to that team member when they are trying to obtain information regarding incident detection software. In the strategies and recommendations in this chapter, strategies are provided to improve information storage in order to improve team learning.

11.3 Project Findings

In this section, we report findings relevant to learning gathered from interviews, focus groups, and surveys of CSIRT professionals.

11.3.1 FINDINGS RELEVANT TO CREATIVITY AND CURIOSITY

Creativity is essential for CSIRT analysts. We surveyed 88 CSIRT employees and asked them to rank the importance and necessity of various knowledge, skills, abilities and other attributes (KSAOs). 85% of the CSIRT analysts rated, “ability to generate novel and useful ideas, for the development of improved processes, services, or products” as important to being effective as a CSIRT analyst and 91% of the CSIRT analysts rated the “ability to be unconventional in thinking and bold in new ideas” as important for success. When CSIRT analysts think outside the norm to generate novel ideas, they are being creative.

> **“Everyone in my group maintains their expertise by constantly studying, being part of the listservs, answering questions as well as asking them.”**
>
> **~ CSIRT Member**

This project also conducted cognitive task analyses to determine necessary cognitive abilities for CSIRT employees to complete their tasks. Interviewers asked CSIRT members to explain how they made decisions during past experiences. Of the 28 CSIRT CTA interviewees, 79% said statements that indicated the "ability to identify problems in the way that a situation is being handled and generate a set of alternative actions to anticipate novel or unusual events" was important in identifying and mitigating a cybersecurity incident. Creativity is needed by CSIRT members to generate a set of alternative actions, particularly when addressing novel events. Similarly, 46% of CSIRT members identified "creating new or novel ideas and explanations as to why something is happening" as important. When CSIRT members encounter new incidents, creativity is likely necessary to mitigate the issue.

> **“...experience to understand how networks and communications and other systems interact with each other. I mean it’s solving a puzzle is what it is. So you have to have somebody that’s going to be naturally curious, I guess, and want to solve that puzzle. ”**
>
> **~ CSIRT Member**

Our findings indicate that curiosity is important for cybersecurity work. However, in our review of previous sources of information about the personal attributes needed for CSIRT work (i.e., 111 cybersecurity-relevant job ads, 11 relevant position descriptions in the Occupational Informational Network Online, O*NET--see https://www.onetonline.org/), and attributes identified by the National Initiative for Cyber Security Education (NICE) Framework (see http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf), curiosity was not mentioned as an important attribute for CSIRT work; these sources tended to focus on technical abilities almost exclusively. In turn, we concluded that prior work has not included social and psychological characteristics of CSIRT professionals which are critical for effective performance.

Of the 43 focus groups that we conducted, 99% made statements indicating the importance of the “ability to explore unfamiliar topics in order to learn something new or seek out new challenges.” This ability, and the act of exploring to learn, directly relates to curiosity. Similarly, in a survey of cybersecurity analysts, 80 out of 84 (95%) rated the “ability to explore novel, complex, or ambiguous solutions when confronted with a situation (e.g., solving a puzzle)” as important. When CSIRT analysts are curious, they are more likely to explore topics and try new or novel solutions, which may ultimately relate to more CSIRT success in mitigating incidents.

11.3.2 FINDINGS RELEVANT TO NETWORKING

Networking was mentioned in a large number of focus groups and interviews; 53% of the focus groups indicated the importance of "communicating with others outside of the immediate CSIRT (e.g., clients, customers, and constituencies)," although this was not specifically networking for learning purposes. CSIRT managers were more likely than individual analysts to mention networking, with three managers reporting that they specifically send CSIRT members to conferences so they can connect with others. Interestingly, there was some suggestion that the importance of

> **“They have an innate curiosity. They’re not satisfied with just being told, ‘this is the way you do it; therefore, that’s how you do it all the time.’ Let’s go test this. Let’s actually go poke at this a little bit more. Again, questioning the nature of things is a huge piece of it.”**
>
> **~ CSIRT Member**

> **“[This work] is solving a puzzle... So you have to have somebody who’s going to be naturally curious, and want to solve that puzzle.”**
>
> **~ CSIRT Member**

professional networks and networking behaviors may be viewed differently across organizations and across national cultures. We do not, however, have sufficient data from a wide variety of cultures to make this conclusion.

In terms of the skills required to network with others, 81 out of 85 CSIRT members (95%) rated the “skill of understanding others and being understood by others, including speaking, writing, and listening” as important. These basic communication skills are essential for communicating clearly with others and for effective networking (Porter & Woo, 2015). Additional information on networking is provided in Appendix H.

11.3.3 FINDINGS RELEVANT TO TEAM LEARNING

Team learning was frequently mentioned in the focus groups as a key factor for effective CSIRTs. Sharing, storing, and retrieving were all considered important steps in team learning and effectiveness. Across all the teams interviewed, 65% indicated that sharing within their team, the assessment of identified threats, exchanging information, and reaching agreement about how to categorize identified incidents were necessary aspects of CSIRTs’ work. After–action reviews, as well as documenting team members’ actions into a case summary, were mentioned in 42% of the focus groups. These sharing and storage behaviors would likely result in better retrieval of relevant information within the CSIRTs when mitigating a similar incident in the future.

The processes mentioned above may often be associated with learning, although it is important to consider situations in which these processes are independent of learning. For example, information exchange and sharing only lead to learning if other CSIRT members do not already know the information. Another caveat comes in the process of reaching agreement, where individual team members learning via others' viewpoints and the team developing a shared understanding do not necessarily require new information to be introduced.

11.4 Strategies and Recommendations

To create a learning climate conducive to individual, team and MTS levels, we offer several strategies. These strategies include the selection of individuals for cybersecurity work based on learning-related skills, designing work to promote learning and development, leader behaviors to encourage learning, and training activities to strengthen learning practices. Within each strategy, we recommend one or more ways of creating a learning climate that have been shown to be effective in the organizational sciences literature.

11.4.1 STRATEGY 1: SELECTION OF INDIVIDUALS WHO ARE CREATIVE AND CURIOUS

Creativity and curiosity are considered to be relatively stable characteristics of individuals, but they vary across different situations. Further, creativity and curiosity can be changed through developmental activities. One strategy that managers can implement to improve creativity and curiosity among their team members is to select individuals who are creative and curious.

> **“You know, the concept of ‘lessons learned’ is hopefully we’re learning something out of it. So we try and at least ask the question: What are the action items that come out of this? What did we learn – positive and negative – out of this?”**
>
> **~ CSIRT Member**

Alternatively, managers can promote creative and curious behavior among their team members through their own behaviors (e.g., role modeling), as described in the next section.

Curiosity and creativity are strongly related to each other; in some studies, the empirical relation between the two was strong enough to suggest that creativity and curiosity may be redundant (Hahn, Lee, & Lee, 2015). Curiosity, however, results in information-seeking and leads to learning, while creativity leads to

> **“…being part of the cybersecurity team, it’s also very important to understand the other companies. If you speak with a financial institution…with certain managers or people or groups, they really don’t have a clue how ISP operates and what the issues of an ISP are. Yeah, we share the same customers, but from a technology perspective, from a capability perspective, from understanding how all the parts of the business works even with the companies that are completely different than the technical parts.”**
>
> **~ CSIRT Member**

learning through exploration of novel directions and modifying and extending known solutions. Both curiosity and creativity lead to information-seeking and result in learning. For example, in one study, creativity resulted in a 42% increase in learning (Eschleman, Madsen, Alarcon, & Barelka, 2014).

Hiring people who are creative and curious might be one approach for increasing the information-seeking behaviors of a CSIRT. Selection of job applicants could be based on previous experience, structured interview questions, or responses to a psychological test. For example, during the selection process, applicants could be asked to describe previous instances where they were creative at work, or how and why they would describe themselves as curious. One caveat to asking an applicant to describe previous work experience in which they demonstrated creativity and curiosity is the presumption that the individual has had the opportunity to demonstrate creativity and curiosity in previous positions. Alternatively, one could ask applicants what they would do in a given hypothetical situation, through which it would be possible to demonstrate a more creative or curious response versus a less creative or curious response (see Chapter 5 "Communication Effectiveness in Incident Response," for more discussion of situational interviewing). Some of the assessment items provided at the beginning of this chapter for creativity and curiosity might serve as the basis for interview questions. Lastly, there are also psychological measures of curiosity that might be used for assessing applicants.

Employee selection processes need to be properly validated before using them in an employment selection procedure. **Thus, we do not suggest that managers start using selection procedures for identifying applicants who are creative and curious until a proper employment validation study is conducted to ensure that the procedure is legally defensible.** Please see Appendix C for general guidelines on how to conduct such a selection validation study (Note: it is strongly recommended that a trained organizational psychologist be hired to conduct such a study).

11.4.2 STRATEGY 2: LEADER BEHAVIORS TO ENCOURAGE LEARNING

Recommendation 1. Engage employees' creativity and curiosity

Leaders can influence a situation to either encourage or discourage creative and curious behaviors of CSIRT professionals. In other words, leaders can create a learning climate where individuals or teams are encouraged to seek new information, develop new skills, and engage in creative problem-solving. One of the managers who we interviewed indicated that he deliberately assigned some of the analysts to work on special development projects, allowing them to show their creativity. This manager said that he made this decision, at least in part, based on the analysts previously exhibiting curiosity through their work. This is an example where the leader arranged the situation to encourage creativity and curiosity.

The organizational science literature provides other examples of how leaders can increase employees' learning. For example, managers can encourage CSIRT professionals to self-assess their own levels of curiosity and creativity. Based on self-assessment, they can plan their own learning activities, which can lead to greater task knowledge, increased confidence, and better performance, through increased creativity and curiosity. In one study, seeking new information for its own sake, rather than merely to demonstrate mastery (i.e., being curious), explained about 7% of employees' ability to transfer learning to a more complex task, and the types of learning strategies they used explained 28% of their ability to transfer learning (Ford, Smith, Weissbein, Gully, & Salas, 1998). In another study, there was a 69% likelihood (as opposed to the 50% expected by chance) that employees whose managers encouraged them to be more creative and curious by setting goals for improving performance (developmental objectives) and pursuing developmental opportunities (e.g., certification courses) would demonstrate feedback-seeking behaviors more than those employees not given that encouragement; there was also a 67% likelihood (as opposed to the 50% expected by chance) that encouraged employees would be more communicative regarding errors they had made. Also in that study, taking a developmental approach was more effective when the employees were rewarded for learning new skills and knowledge (Chughtai & Buckley, 2010).

Recommendation 2. Facilitate reflection in teams (team reflexivity, or team reflections, and adaptation)

To increase team learning, teams should assess their past, present, and future strategies and processes (Schippers, West, & Dawson, 2015; Wilson et al., 2007). Thinking about and discussing whether the team is working effectively (i.e., team reflexivity), and ways to improve their performance, can lead to the adaptation of existing strategies and processes or the development of new strategies and processes. Studies have found a relationship between team reflexivity and new ideas. For example, one study on health care teams found that there is a 70% likelihood (as opposed to the 50% expected by chance) that a team will report a higher number of new processes, procedures, and ideas when they regularly engage in team reflexivity, than if the team is not engaged in those discussions regularly (Schippers et al., 2015). If the team as a whole gains a new understanding of processes, procedures, or ideas as a result of planning and reflection, then team learning has occurred.

Managers are responsible for getting team members to reflect on events and identify where changes are needed. This, in turn, can increase performance and team effectiveness. One study of managers found that there is a 68% likelihood (as opposed to the 50% expected by chance) that team members will partake in team reflection and adaptation, which increases team performance, when their leader establishes a shared vision among team members compared to when the leader does not (Schippers, Den Hartog, Koopman, & van Knippenberg, 2008). Beyond promoting reflection on and assessment of events, managers can also influence learning by guiding and promoting change. For example, one study found that when leaders provide followers with intellectual stimulation and inspiration, continuous learning is facilitated at the individual, team and organizational level (Garcia-Morales, Jimenez-Barrionuevo, & Gutierrez-Gutierrez, 2012).

Team reflexivity enhances learning because teams discuss and reach a shared understanding about how they can improve processes and complete tasks in new ways. These reflective strategies can result in a change, or improvement, in the shared understanding among team members of how they should interact on team tasks, thus promoting team learning. For more on developing a shared understanding, see Chapter 8, "Shared Knowledge of Unique Expertise."

Recommendation 3. Provide feedback in debriefings (after-action reviews)

Debriefings, also referred to as after-action reviews, can provide the setting for teams to reflect upon and adapt their processes. Debriefing should occur after an incident, or after a practice exercise, and can be as little as 5 to 10 minutes in length. Debriefings provide team members the opportunity to identify issues so that the team is able to learn from the issues and change their behaviors for future incidents. Debriefings can be unguided or guided. For the 12 principles of effective debriefings, please see Strategy 4 in Chapter 7, "Collaborative Problem Solving in Incident Response."

An important part of the debriefing process that we will discuss here is feedback. Feedback should be provided at the end of a task and in a timely manner (Sessa & London, 2008). Previous research suggests that when providing feedback, one should allow for a slight delay (as little as 8 minutes), which provides individuals with time to process what they have learned and results in better long-term retention of new information. A study on information retention showed that there is a 61% likelihood (as opposed to the 50% expected by chance) that individuals will better retain learned information when the feedback is slightly delayed than if it is given immediately (Smith & Kimball, 2010).

Feedback is important for initial learning and also for retention of learning. Missed opportunities for feedback and debriefings may hamper learning substantially. Feedback should promote accomplishments but also discuss failures. Specifically, feedback should focus on how goals were set, tracked, and reached as well as how team members coordinated, communicated, structured and solved problems, and if members felt free to express their opinions. For more information on debriefings and feedback, please refer to Chapter 7, "Collaborative Problem-Solving in Incident Response."

Recommendation 4. Promote trust and respect among team members

For team learning to occur, agreement must be reached among team members about new understandings of knowledge, behaviors, or routines (Wilson et al., 2007). Team members must all agree and share a commitment to change their routine if changes are to occur. A team reaching agreement regarding new, or changes to existing, knowledge and behaviors indicates that the team has the capacity for “sharing” to be effective and promote team learning.

Mutual respect and trust within the team creates a safe environment where people are comfortable being themselves and sharing their thoughts (Edmondson, 1999). This safe climate encourages team members to raise new ideas and share thoughts on changes to routines, objectives and behaviors, which promotes team learning. This psychological safety climate is the strongest influence on team learning behavior, over and above team cohesion, interdependence and the team's belief in its own effectiveness (Van den Bossche, et al., 2006). Research has shown that there is an 82% likelihood (as opposed to the 50% expected by chance) that team members will perceive the organization as being more tolerant of failure as part of the learning process when team members believe there is a high amount of psychological safety rather than if they believe there is a low amount (Carmeli, 2007). This finding suggests that psychological safety is necessary in allowing employees to feel comfortable learning from making errors (See Recommendation 10, in this chapter, on Error Management). For strategies to improve psychological safety and trust please see Chapter 9, "Trust in Teams and Incident Response Multiteam Systems." That chapter provides team building activities and ways to empower team members to work together.

11.4.3 STRATEGY 3: DESIGN WORK TO ENHANCE LEARNING AND DEVELOPMENT

Work design refers to “the content and organization of one’s work tasks, activities, relationships and responsibilities” (Parker, 2014, p. 662) and has been demonstrated to affect workers’ motivation, safety and health, as well as their learning and development (Parker, 2014). For this section we are focusing on work design aspects that promote learning and development.

> **“In cybersecurity, nothing should be repetitive. If something is repetitive, then we have a bigger, underlying problem. If the same incident happens over and over again, so where's the infection vector, why isn't this infection vector fixed, right? So, after every case we have the lessons learned. After at least every [severity] one and [severity] two case, or the high priority cases, we have a lessons learned where we look why did this happen, how can we avoid it to happen again? If you have something that's very repetitive in security, you should definitely look into why it is happening that often.”**
>
> **~CSIRT member**

Recommendation 5: Improve work design to enhance learning

Work roles are often designed without careful consideration of the effects on individuals in those roles. The following principles of work design (Parker, 2014) can improve CSIRT professionals' learning and development:

- Allow CSIRT analysts autonomy in their work roles so that they have influence over their work, working methods and pace of work (to the extent possible). Research has shown that there is a 68% likelihood (as opposed to the 50% expected by chance) that employees will learn a new task and transfer those skills to a different task setting better if they are given a high amount of autonomy in their work than if they are given a low amount of autonomy (Wielenga-Meijer, Taris, Wigboldus, & Kompier, 2010).
- Design cybersecurity work roles so that analysts have (a) a variety of tasks using a range of skills, and (b) the opportunity to develop new skills. Previous research has shown that increasing the variety of skills used accounts for almost 10% of job performance improvement, including the learning component of job performance (Morgeson, Delaney-Klinger, & Hemingway, 2005).
- Design work roles so that interdependent tasks are combined into a single work role, and combine interdependent work roles into a team's work role. Interdependence among tasks (i.e., various team members' tasks depend on one another's) has an 86% likelihood (as opposed to the 50% expected by chance) of resulting in higher team learning compared to teams who do not have task interdependence (Van den Bossche et al., 2006).

> **“I guess that's the reason why we work so well together, because as a group, we understand each other.”**
>
> **~CSIRT Leader**

Recommendation 6. Put in place mentoring programs

Participation in mentoring programs for CSIRT members can help CSIRT professionals to identify networking and learning opportunities and resources (e.g., Bower, 2007; Cawyer, Simonds, & Davis, 2002). Participation in mentoring programs promotes the acquisition of knowledge, skills, and abilities (Ramaswami & Dreher, 2007). This learning typically occurs by the mentor providing challenging assignments, coaching the protégé, and role modeling. Mentoring is an especially useful tool for learning for organizational newcomers (Ostroff & Kozlowski, 1993) and also can be especially important in complex work. Based on a review of the mentoring literature, employees who had a mentor reported 11% higher competence and skill development than people who did not have mentors (Eby, Allen, Evans, Ng, & DuBois, 2008).

Organizational science research, as summarized by Finkelstein and Poteet (2007), suggests these best practices for formal mentoring programs:

- Management should support mentoring programs and make sure that participants understand that management supports these programs.
- The mentoring program will need to be tailored to the specific organization's goals relative to learning and development. In the CSIRT environment, this could include learning in the technical cybersecurity domain and learning in network development and maintenance.
- Generally, mentors and protégés should be assigned to each other based on the purpose of the program. For example if the purpose of the mentoring program is to increase knowledge about different cybersecurity threats, mentors and protégés with diverse backgrounds should be matched.
- Clear objectives need to be specified for the mentoring program. For example, is the intent of the program for protégés to learn about their own organization, learn about cybersecurity developments outside of the CSIRT, or learn who has specific expertise that is relevant to responding to incidents?
- Training for mentors is recommended before they participate in a formal mentoring program.
- Generally, the protégé should have some input into who the mentor will be, although research findings are not consistent on this.

11.4.4 STRATEGY 4: TRAINING

Recommendation 7. Train for networking skills

Networking can increase the size of one's professional network, the strength of the relationships in one's network, the number of connections in one's network, and the resources and information in one's network (Porter & Woo, 2015). Access to information facilitates learning, and engaging in networking behaviors can provide CSIRT professionals access to valuable information. Networking is not necessarily difficult to do; yet, it is not something that everyone enjoys doing or is adept at in the professional context.

Training in interpersonal and relationship building skills can improve CSIRT professionals' ability to network both within their organization and outside of their organization (De Janasz & Forret, 2008). According to Conjar (2014, p. 12), these relationship-building skills include the following (also see de Janasz & Forret, 2008; McCauley & Douglas, 2004; Uhl-Bien & Maslyn, 2003):

- Oral communication;
- Active listening;
- Building trust; and,
- Creating rapport.

Organizational research finds that networking ability accounts for developmental growth. One study of the development of managers found that networking ability resulted in a 25% increase in developmental growth (Conjar, 2014).

Recommendation 8. Train CSIRT professionals on how to establish a professional developmental network

CSIRT professionals, in addition to the interpersonal skills mentioned in Recommendation 7 above, need to understand what they should be looking for in their professional developmental network. There are three factors that need to be considered in establishing a professional network for developmental purposes (McCauley & Douglas, 2004):

1. Assessment: Members in the network need to be able to provide relevant information and provide the individual with feedback on their developmental progress.
2. Challenge: Members of the network need to be able to get individuals to move beyond their normal comfort zones, often referred to as "stretch experiences."
3. Support: Members in the network should be supportive, helping individuals manage the challenges faced when increasing their knowledge, skills, and abilities.

There is a tendency for people to approach others who are similar to themselves. Doing so does not yield a sufficiently diverse network if one is seeking to learn from the people in the network. Learning is increased by almost 25% when the members of the developmental network are from different organizational functions (e.g., IT, marketing, finance; Conjar, 2014). This indicates that CSIRT professionals need to network with people from other backgrounds, as well as from varied cybersecurity backgrounds, to optimize the type of information available.

Recommendation 9. Guided discovery learning

Managers can facilitate the process of team learning through training activities that provide teams with the opportunity to share and store knowledge, behaviors, and processes. In training activities, teams are able to try new things and make errors along the way without the potentially negative consequences that experimentation and errors could have during real CSIRT incidents.

In discovery-based activities, teams actively participate in their learning activities. In comparison to more traditional learning approaches (e.g., lectures, videos, or manuals), active learning gives the learners control over their own instructional processes and experiences (Bell & Kozlowski, 2008). Trainees should be able to "discover" new rules and ideas. Instead of the passive receipt of knowledge from external sources (e.g., teachers, texts), team members in active learning receive few instructions to complete a task and, as a result, must explore and experiment to find the strategies that are most effective. Active learning does not simply mean, however, that team managers should not provide any instruction. Rather, the formal training design of these seemingly unstructured activities influences the team's processes for focusing their attention and effort. Learners construct their own understandings through experimentation and exploration, which better promotes an increase in learning and comprehension compared to more passive learning approaches. Active learning not only can facilitate individual learning, but also team learning because these activities provide teams with opportunities to share information and strengthen their sharing processes.

Discovery learning can be structured in various ways. There is unguided discovery learning, where learners receive little to no guidance or feedback from an instructor or manager. Research, however, has found that this type of unassisted discovery was not more effective in post-tests or content recall compared to traditional learning activities (Alfieri, Brooks, Aldrich, & Tenenbaum, 2011; Mayer, 2004).

Discovery learning can also be guided exploration such that individuals' self-directed learning is supplemented with guidance to focus their thinking processes and behaviors in productive directions. For instance, in an exploratory learning activity, learners would not be directly given the solutions to the task or the rules. Although they have minimal structure on the task, learners receive some external guidance to help guide their thinking and behaviors. One form of external guidance could be a list of learning objectives, such as the skills and strategies learners are to develop through the training. Such guided discovery learning does not necessarily improve training performance on that specific task but does result in improved performance on other tasks where they could adapt their performance (Bell & Kozlowski, 2008). Results suggest a 54.5% likelihood (as opposed to the 50% expected by chance) that guided discovery learning yields higher performance in adaptive transfer tasks compared to passive learning. Much of CSIRT work aligns with adaptive transfer tasks, as the tasks and incidents that occur after training will likely not be the exact incident or tasks presented in training. CSIRTs are dynamic and events are always changing. Thus, active learning is best for CSIRT members to develop the skills during training that will help them adapt, recognize, and respond to changes in the CSIRT environment.

Guided discovery helps the trainees activate thinking patterns and knowledge necessary to solve the current problem. Additionally, when trainees are made aware of the appropriate knowledge base relative to the task being trained, they are able to integrate this new information and better understand the material. When trainees do not have any guidance, it is possible that they will never learn the knowledge that the training was intended to teach.

Guided discovery learning is a mix of guidance and exploration. To structure guided exploratory learning (Bell & Kozlowski, 2008; Bell & Kozlowski, 2002; Mayer, 2004):

1. Instructors or leaders must provide the team with a task.
   - The sequencing of the task should involve more fundamental material early on, followed by more strategic planning elements.
2. Learners need to have control over many aspects of the task, such as the pace of conducting the task.
3. The trainers need to continually provide guidance on the following:
   - Task sequence – The task should start with more basic concepts first and then move to more complex concepts. Providing trainees with guidance on the basic processes necessary to solve the problem without giving the solution can be useful.
   - Direction on strategy development – After basic skill

acquisition, trainees should be guided toward consideration of strategic task aspects that contribute to more advanced expertise.

- Cognitive modeling
  - Show trainees where they should allocate their attention. Guidance helps trainees determine what they should be studying and provides them with additional information about what they should pay attention to and what level of effort to exert.
- Systematic and pre-planned exploration
  - Provide guidance to help trainees regulate their learning in terms of what to study and what to practice.
- Feedback is given, including specific information about the extent to which the trainee has learned each of the concepts.

Guided discovery learning and error management training (see next section) are both forms of active learning. Please see Appendix D, Programs of Instruction for CSIRT Training, for an integrated guide for conducting guided discovery training and error management training.

Recommendation 10. Error management training

Error management training assumes that, within the context of active learning, errors serve as useful learning tools by helping trainees identify learning gaps (Ivancic & Hesketh, 1995). Such training focuses not as much on preventing error occurrence during performance trials, but, instead, on encouraging active learning processes that are more likely to produce early performance errors. Thus, error management training targets post-error learning processes by helping trainees gain skills and knowledge from addressing performance errors (Frese et al., 1991). According to Carter and Beier (2010, p. 672), characteristics of good error management include "communication about errors, sharing error knowledge, helping in error situations, swift error detection and damage control, analyzing errors, coordinating error handling, and fast error handling (Van Dyck, Frese, Baer, & Sonnentag, 2005)."

Error management training is a targeted way to increase the sense of safety from embarrassment, rejection, and punishment from other members of the team (e.g., psychological safety) and is an effective training strategy. A review of 20 error management training studies found that 70% of the time such training methods improved post-training performance (Keith & Frese, 2008). Research has also shown that there is a 77% likelihood (as opposed to the 50% expected by chance) that a firm will perform better financially when there is a strong error management culture than when there is a weak error management culture (van Dyck, et al., 2005)

Error management training typically includes the following:

- Allowing for open exploration of strategies to solve problems, especially during training. Trainees should be allowed to identify and solve errors themselves, rather than having their mistakes pointed out and corrected.
- Removing the concepts of "guilt" and "shame" that are associated with errors. This includes accepting that, in a CSIRT environment, occasional errors are inevitable and present an important chance for the whole team to learn.
- Framing mistakes and learning opportunities for the individual and the team. Treating a mistake as a chance to learn something new will increase psychological safety and reduce the likelihood that an error will be repeated.
- Motivating team members to reframe their ideas about making mistakes. Changing the presumption that errors are only negative and must be avoided to the idea that errors are inevitable, potentially negative, but can be turned into a positive experience (Frese & Keith, 2014).

This strategy can be especially useful for newer CSIRTs, or for those exhibiting low levels of trust, reduce process loss and inefficient incident response processes. Error management training should be used in CSIRTs where managers and leaders have a sufficient amount of time to actually implement this training strategy. Though time-consuming, error management training can greatly benefit team learning. See more detailed guidance on implementing an error management training program in Appendix D, Programs of Instruction for CSIRT Training.

11.5 Chapter Summary

As CSIRTs exist in ever-changing, uncertain, complex, and ambiguous environments, learning is necessary for employees to develop novel solutions, share information, and reach a collective team understanding of new information in order to improve CSIRT performance (e.g., improving quality and speed of responses to incidents). If CSIRT members are creative and curious, they may be more likely to develop new techniques, tools, and solutions to problems. Sharing new techniques, ideas, and changes with people within and outside of the team will spread the ideas of one individual to others. While it demonstrates progress when new knowledge expands from one individual to an entire team or network, it must be taken one step further. These ideas need to be stored in a way that they can be retrieved later, through mental models and/or knowledge databases. To facilitate the sharing of information for team learning, as well as aspects of individual learning such as creativity, it is important for team members to be in a safe environment where they feel free to share ideas and feel that their team can effectively complete their tasks.

When considering the many recommendations we provided to facilitate learning in CSIRTs, it is important to evaluate the costs and benefits of these strategies. Managers' actions are important in promoting learning by their team, such as engaging employees' creativity and curiosity and facilitating reflection on activities. The most important of these managerial behaviors is to provide feedback. Feedback improves team performance and the recall of learned information. To make the most of this feedback and promote CSIRT members' growth, managers should create an environment that is psychologically safe. Team members should feel safe and comfortable in order to share ideas and learn from one another. Such strategies to promote learning are not costly to CSIRTs because managers can accomplish these outcomes simply by changing their own behavior.

Additionally, managers can facilitate learning through various adjustments to work design. These design changes include a mix of increasing autonomy while also increasing task interdependence among team members, providing that these changes in work design do not influence the amount of work that needs to be accomplished. These changes are a cost effective way to improve team learning outcomes. Autonomy will provide the team members with the freedom to learn new material, while team members' reliance on one another to complete their tasks will promote learning within the team. Managers should consider the cost of the time necessary to change and rearrange work assignments so that workers have more flexibility to try new solutions and learn new techniques.

A more costly strategy to improve learning is training, such as guided discovery learning and error management training. These methods will encourage CSIRT members to learn through mistakes as well as trial and error. However, this training requires time to administer, and will take CSIRT members away from their tasks at hand to participate in these training activities. CSIRT managers should take these costs into consideration when deciding which strategies to implement. We encourage managers to first try changes to their own behaviors and actions (e.g., giving feedback, building psychological safety), as well as somewhat easier changes to the roles of employees (e.g., autonomy, interdependence), prior to trying to implement these types of training sessions.

References

Ackerman, P. L., Kanfer, R., & Goff, M. (1995). Cognitive and noncognitive determinants and consequences of complex skill acquisition. *Journal of Experimental Psychology: Applied, 1*, 270–304.

Alfieri, L., Brooks, P. J., Aldrich, N. J., & Tenenbaum, H. R. (2011). Does discovery-based instruction enhance learning? *Journal of Educational Psychology, 103*(1), 1-18.

Amabile, T.M. (1988). A model of creativity and innovation in organizations. Research in Organizational Behavior, 10, 123–167.

Anderson, M. D. (2008). Social networks and the cognitive motivation to realize network opportunities: A study of managers' information gathering behaviors. *Journal of Organizational Behavior, 29*, 51-78.

Armstrong-Stassen, M. & Schlosser, F. (2008). Benefits of a supportive development climate for older workers. *Journal of Managerial Psychology, 23*(4), 419-437.

Bell, B. S., & Kozlowski, S. W. J. (2002). Adaptive guidance: Enhancing self-regulation, knowledge, and performance in technology-based training. *Personnel Psychology, 55*(2), 267-306.

Bell, B. S., & Kozlowski, S. W. (2008). Active learning: effects of core training design elements on self-regulatory processes, learning, and adaptability. *Journal of Applied psychology, 93*(2), 296-316.

Bower, G.G. (2007). Factors influencing the willingness to mentor 1st-year faculty in physical education departments. *Mentoring & Tutoring, 15*(1), 73-85.

Cacioppo, J.T., Petty, R.E., & Kao, C.F. (1984). The efficient assessment of need for cognition. *Journal of Personality Assessment, 48*(3), 306-307.

Carmeli, A. (2007). Social capital, psychological safety and learning behaviours from failure in organisations. *Long Range Planning, 40*, 30-44.

Cawyer, C.S., Simonds, C., & Davis, S. (2002). Mentoring to facilitate socialization: The case of the new faculty member. *International Journal of Qualitative Studies in Education, 15*(2), 225-242.

Chen, T. R., Shore, D. B. Zaccaro, S. J., Dalal, R. S., Tetrick, L. E. & Gorab, A. K. (2014). An organizational psychology perspective to examining computer security incident response teams. *IEEE Security Privacy, 5*, 61-67.

Chughtai, A. A., & Buckley, F. (2010). Assessing the effects of organizational identification on in-role job performance and learning behaviour: The mediating role of learning goal orientation. *Personnel Review, 39(*2), 242-258.

Conjar, E. A. (2014).The influence of social networks on development: An empirical examination of leadership development. ProQuest Dissertations Publishing, 3671719.

Cross, R. & Thomas, R. (2008). How top talent uses networks and where rising stars get trapped. *Organizational Dynamics, 37*, 165-180.

de Janasz, S. C., & Forret, M. OL. (2008). Learning the art of networking: A critical skill for enhancing social capital and career success. *Journal of Management Education, 32*, 629-650.

Dweck, C.S. (1986). Motivational processes affecting learning. *American Psychologist, 41*, 1040-1048.

Eby, L. T., Allen, T. D., Evans, S. C., Ng, T., & DuBois, D. L. (2008). Does mentoring matter? A multidisciplinary meta-analysis comparing mentored and non-mentored individuals. *Journal of Vocational Behavior, 72*, 254-267.

Edmondson, A. C. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly, 44*, 350-383.

Egan, T.M., Yang, B., & Bartlett, K.R. (2004). The effects of organizational learning culture and job satisfaction on motivation to transfer learning and turnover intention. *Human Resource Development Quarterly, 15*(3), 279-301.

Ellis, A. P. J., Hollenbeck, J. R., Porter, C. O. L. H., Ilgen, D. R., West, B. J., & Moon, H. (2003). Team learning: Collectively connecting the dots. *Journal of Applied Psychology, 88*, 821–835.

Eschleman, K. J., Madsen, J., Alarcon, G., & Barelka (2014). Benefiting from creative activity: The positive relationships between creative activity, recovery experiences, and performance-related outcomes. *Journal of Occupational and Organizational Psychology, 20*, 579-598.

Finkelstein, L. M. & Poteet, M. L. (2007). Best practices in workplace formal mentoring programs. . In T. D. Allen and L. T. Eby (Eds.). *The Blackwell Handbook of Mentoring: A Multiple Perspectives Approach*. pp. 345 – 367. Malden, MA: Blackwell Publishing.

Ford, J. K., Smith, E. M., Weissbein, D. A., Gully, S. M., & Salas, E. (1998). Relationships of goal orientation, metacognitive activity, and practice strategies with learning outcomes and transfer. *Journal of applied psychology, 83*(2), 218-233.

Forret, M. L., & Dougherty, T. W. (2004). Networking behaviors and career outcomes: differences for men and women? *Journal of Organizational Behavior, 25*(3), 419-437.

Frese, M., Brodbeck, F.C., Heinbokel, T., Mooser, C., Schleiffenbaum, E., & Thiemann, P. (1991). Errors in training computer skills: On the positive function of errors. *Human-Computer Interaction, 6*, 77-93.

Frese, M. & Keith, N. (2014). Action errors, error management, and learning in organizations. *Annual Review of Psychology, 66*, 661-687.

Garcia-Morales, V.J., Jimenez-Barrionuevo, M.M., & Gutierrez-Gutierrez, L. (2012). Transformational leadership influence on organizational performance through organizational learning and innovation. *Journal of Business Research, 65*, 1040-1050.

Govaerts, N., Kyndt, E., Dochy, F., & Baert, H. (2011). Influence of learning and working climate on the retention of talented employees. *Journal of Workplace Learning, 23*(1), 35-55.

Hahn, M. H., Lee, K. C., & Lee, D. S. (2015). Network structure, organizational learning culture, and employee creativity in system integration companies: The mediating effects of exploitation and exploration. *Computers in Human Behavior, 42*, 167-175.

Harrison, S.H., Sluss, D.M., & Ashforth, B.E. (2011). Curiosity adapted the cat: The role of trait curiosity in newcomer adaptation. *Journal of Applied Psychology, 96*(1), 211-220.

Hofmann, D.A. & Frese, M. (2011). Errors, error taxonomies, error prevention and error management: Laying the groundwork for discussing errors in organizations. In Frese, M. & Hofmann, D. (Eds.), *Errors in organizations*. Society for Industrial and Organizational Psychology Frontier Series.

Ivancic, K. & Hesketh, B. (1995). Making the best of errors during training. *Training Research Journal, 1*, 103-125.

Keith, N. & Frese, M. (2008). Effectiveness of error management training: A meta-analysis. *Journal of Applied Psychology, 93*(1), 59-69.

Litman, J. A. (2008). Interest and deprivation factors of epistemic curiosity. *Personality and Individual Differences, 44*, 1585–1595.

Marsick, V.J. & Watkins, K.E. (2003). Demonstrating the value of an organization's learning culture: The dimensions of organization questionnaire. *Advances in Developing Human Resources, 5*(2), 132-151.

Mayer, R. E. (2004). Should there be a three-strikes rule against pure discovery learning? *American Psychologist, 59*(1), 14-19.

McCauley, C.D. & Douglas, C.A. (2004). Developmental relationships. In C.D. McCauley & E. Van Velsors (eds.) *The Center for Creative Leadership Handbook of Leadership Development*, 2nd Ed, (pp. 204-233). San Francisco, CA: Jossey-Bass.

McFadyen, M, & Cannella, A. (2004). Social capital and knowledge creation: Diminishing returns of the number and strength of exchange relationships. *Academy of Management Journal, 47*, 735-746.

Morgeson, F. P., Delaney-Klinger, K., & Hemingway, M. A. (2005). The importance of job autonomy, cognitive ability, and job-related skill for predicting role breadth and job performance. *Journal of Applied Psychology, 90*(2), 399-406. http://dx.doi.org/10.1037/0021-9010.90.2.399

Mumford, M. D., Antes, A. L., Caughron, J. J., Connelly, S., & Beeler, C. (2010). Cross-field differences in creative problem-solving skills: A comparison of health, biological, and social sciences. *Creativity Research Journal, 22*(1), 14-26.

Mussel, P. (2010). Epistemic curiosity and related constructs: lacking evidence of discriminant validity. *Personality and Individual Differences, 49*, 506-510.

Mussel, P. (2013). Introducing the construct curiosity for predicting job performance. *Journal of Organizational Behavior, 34*(4), 453–472.

Mussel, P. (2011, July). A theoretical framework for the personality of intellectual achievements. Paper presented at the meeting of the International Society for the Study of Individual Differences, London.

Nikolova, I., Van Ruysseveldt, J., De Witte, H., & Van Dam, K. (2014). Learning climate scale: Construction, reliability and initial validity evidence. *Journal of Vocational Behavior, 85*, 258-265.

Oldham, G.R. & Da Silva, N. (2015). The impact of digital technology on the generation and implementation of creative ideas in the workplace. *Computers in Human Behavior, 42*, 5-11.

Ostroff, C., & Kozlowski, S. W. (1993). The role of mentoring in the information gathering processes of newcomers during early organizational socialization. *Journal of Vocational Behavior, 42*(2), 170-183. http://dx.doi.org/10.1006/jvbe.1993.1012

Parker, S.K. (2014). Beyond motivation: Job and work design for development, health, ambidexterity, and more. *Annual Review of Psychology, 65*, 661-691.

Porter, C. M., & Woo, S. E. (2015). Untangling the networking phenomenon: A dynamic psychological perspective on how and why people network. *Journal of Management. 41*, 1477-1500. DOI: 10.1177/0149206315582247

Ramaswami, A. & Dreher, G. F. (2007). The venefits associated with workplace mentoring relationships. In T. D. Allen and L. T. Eby (Eds.). *The Blackwell Handbook of Mentoring: A Multiple Perspectives Approach*. pp. 211 – 231. Malden, MA: Blackwell Publishing.

Ratwani, K.L., Zaccaro, S.J., Garven, S., & Geller, D.S. (2010). The role of developmental social networks in effective leader self-learning processes. In M.G. Rothstein & R.J. Burke (Eds.), *Self-management and Leadership Development*, (pp. 395-426). Celtenham, UK: Edward Elgar.

Reio Jr., T.G., & Wiswell, A. (2000). Field investigation of the relationship among adult curiosity, workplace learning, and job performance. *Human Resource Development Quarterly, 11*(1), 5-30.

Schippers, M. C., Den Hartog, D. N., Koopman, P. L., & van Knippenberg, D. (2008). The role of transformational leadership in enhancing team reflexivity. *Human Relations, 61*(11), 1593-1616.

Schippers, M. C., West, M. A., Dawson, J. F. (2015). Team reflexivity and innovation: The moderating role of team context. *Journal of Management, 41*, 769-788.

Scott, G., Leritz, L. E., & Mumford, M. D. (2004). The effectiveness of creativity training: A quantitative review. *Creativity Research Journal, 16*(4), 361-388.

Sessa, V.I. & London, M. (2008). Interventions to stimulate group learning in organizations. *Journal of Management Development, 27*, 554-573.

Smith, T. A., & Kimball, D. R. (2010). Learning from feedback: Spacing and the delay–retention effect.*Journal of Experimental Psychology: Learning, Memory, and Cognition, 36*(1), 80-95. http://dx.doi.org/10.1037/a0017407

Sørensen, O.H. & Holman, D. (2014). A participative intervention to improve employee well-being in knowledge work jobs: A mixed methods evaluation study. *Work & Stress: An International Journal of Work, Health & Organisations*, 28:1, 67-86.

Sung, S.Y. & Choi, J.N. (2014). Do organizations spend wisely on employees? Effects of training and development investments on learning and innovation in organizations. *Journal of Organizational Behavior, 35*, 393-412.

Uhl-Bien, M. & Maslyn, J.M. (2003). Reciprocity in manager-subordinate relationships: Components, configurations, and outcomes. *Journal of Management, 29*, 511.

Van den Bossche, P., Gijselaers, W. H., Segers, M., & Kirschner, P. A. (2006). Social and cognitive factors driving teamwork in collaborative learning environments team learning beliefs and behaviors. *Small Group Research, 37*(5), 490-521.

Van Dyck, C., Frese, M., Baer, M., & Sonnentag, S. (2005). Organizational error management culture and its impact on performance: A two-study replication. *Journal of Applied Psychology, 90*(6), 1228-1240.

Van Velsor, E. & McCauley, C.D. (2004). Our view of leadership development. In C.D. McCauley & E. Van Velsor (Eds.), *The Center for Creative Leadership Handbook of Leadership Development* (2nd Ed., pp. 1-22). San Francisco, CA: Jossey-Bass.

Wielenga-Meijer, E.G.A., Taris, T.W., Wigboldus, D.H.J., & Kompier, M.A.J. (2010). Costs and benefits of autonomy when learning a task: An experimental approach. *The Journal of Social Psychology, 151*(3), 292-313

Wilson, J.M., Goodman, P.S., & Cronin, M.A. (2007). Group learning. *Academy of Management Review, 32*(4), 1041-1059.

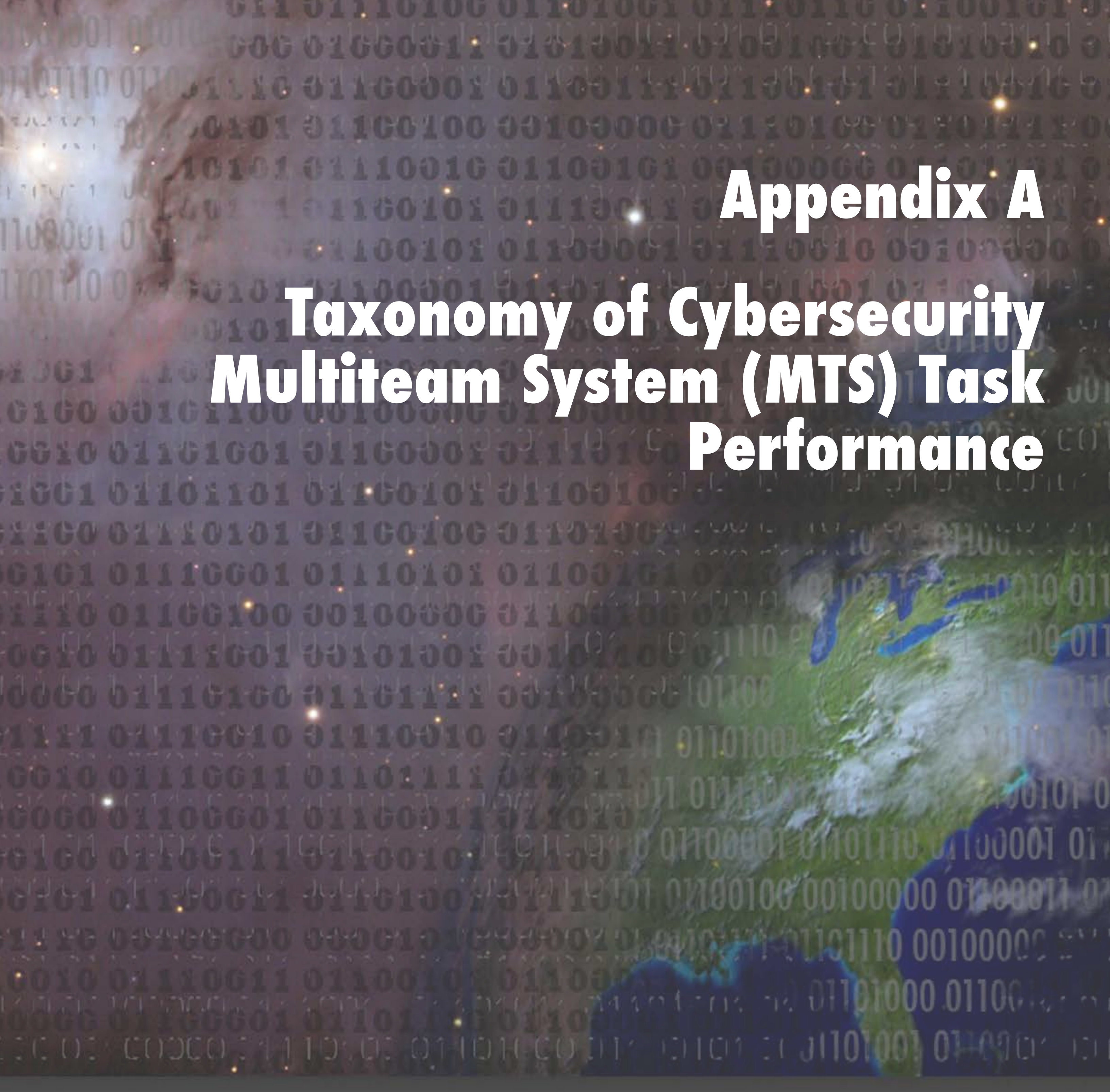
Wolff, H.G. & Moser, K. (2006). Entwicklung and Validierung einer Networkingskala [Development and validation of a networking scale]. *Diagnostica, 52*, 161-180.

Wolff, H.G. & Moser, K. (2009). Effects of networking on career success: A longitudinal study. *Journal of Applied Psychology, 94*(1), 196-206.

Appendices

Appendix A

Taxonomy of Cybersecurity Multiteam System (MTS) Task Performance



Contents

A.1 Introduction

Our initial task in this research effort was to construct a taxonomy of performance activities that are enacted by members of effective cybersecurity incident response teams and multiteams systems. Such a taxonomy can then be used to develop work analysis measures and performance assessment tools. In this document, we provide a brief summary of how we constructed the taxonomy. Zaccaro, Hargrove, Chen, Repchick, and McCauseland (2016) provide an expanded description of its conceptual framework, along with an abbreviated version of the taxonomy.

To guide our taxonomic development, we first reviewed the cybersecurity incident response team literature, which included technical reports (e.g., Alberts, Dorofee, Killcrece, Ruefle, & Zajicek, 2004), peer reviewed articles (Ahmad, Hadgkiss, & Ruighauer, 2012), federal agency announcements (Ruefle, 2008), and best practice recommendations (Brownlee & Guttman, 1998; ENISA, 2010). We also investigated the teams literature from organizational psychology (Fleishman & Zaccaro, 1972; Kozlowski & Ilgen, 2006; Salas, Dickinson, Converse, & Tannenbaum, 1992; Sundstrom, DeMeuse, & Futrell, 1990), as well as incorporated a network perspective of interacting component teams (Mathieu, Marks, & Zaccaro, 2001). After examining extant definitions, we extracted key and/or reoccurring themes, resulting in the following definition (Zaccaro, et al., 2016, p. 24):

> *A cybersecurity [multiteam system] is a collection of two or more teams each of which is composed of two or more individuals interacting with each other, information technology (IT) infrastructure, IT personnel, end users, management, and other component teams to provide proactive and reactive cybersecurity services to support the mission of a defined constituency.*

A.2 Development of Taxonomic Dimensionality

This definition informed the scope of our taxonomic development; that is, we sought to develop a preliminary model that could be used as a starting point for understanding the performance requirements of a cybersecurity incident response multiteam system (CSIRT MTS). To determine the most appropriate dimensionality for the proposed taxonomy, we reviewed extant taxonomies at the individual level (Borman, Ackerman, & Kubisiak, 1994; Borman & Brush 1993; Borman, Bryant, & Dorio, 2010; Hunt, 1996; Peterson, Mumford, Borman, Jeanneret, & Fleishman, 1999; Viswesvaran, 1993) and at the team level (Marks et al., 2001). Based on these reviews, we proposed a multiphase, multilevel framework of CSIRT MTS performance. Specifically, the multiphase element refers to *processes (planning), behaviors (execution), and outcomes (effectiveness),* and the multilevel aspect includes *individual, within team*, and *multiteam systems*. Please see Zaccaro, et al. (2016) for additional details on the dimensional structure for processes and behaviors.

Performance outcomes can be thought of as goal achievement, which is measured as an *output* (e.g., quantity, quality, or customer satisfaction), a *consequence* for constituencies and stakeholders, and/or an increase in *abilities* of an individual, a component team within an MTS, and/or the MTS as a whole (adapted from Wildman, Bedwell, Salas, & Smith-Jentsch, 2011. p. 321). *Individual* performance outcomes involve outputs, consequences, and/or an increase in abilities for individuals. Analogically, *within component team* performance outcomes involve component team- level outputs, consequences, and/or increases in abilities for component teams as a whole. Lastly, *between component team* performance outcomes involve system outputs, consequences, and/or increases in abilities for the multiteam system as a whole.

A.3 Procedure for Taxon Specification

The specification of taxa in the proposed taxonomy was anchored in a theoretical rationale (see Zaccaro, et al., (2016) for more details) and has undergone subsequent revisions. Initial validation studies involved only limited sample sizes; therefore, revisions only included reorganization or addition; no taxa were deleted.

A.3.1 GENERATION OF TAXA

To initially populate the cells articulated above, we relied heavily on extant task performance research across different types of jobs (e.g., Borman et al., 1994; Borman & Brush 1993; Borman et al., 2010; Campbell, 1993, Hunt, 1996; Marks et al., 2001; Peterson et al., 1999) and more context specific sources (e.g., technical CSIRT activities; Alberts et al., 2004). Given the preliminary stage of the research, we opted for inclusivity, meaning that if we felt a taxon had any potential to contribute to future understanding, then we included it in the initial framework.

A.3.2 TAXON VALIDATION

The taxonomy was validated based on responses obtained from (a) some prior research on the nature of cybersecurity jobs that produced what are known as the National Initiative for Cybersecurity Education (NICE) task statements and (b) from interviews with focus groups of individuals working in cybersecurity. These NICE statements are part of the National Cybersecurity Workforce Framework that was developed to identify tasks and knowledge, skills, abilities, and other attributes (KSAOs) needed in cybersecurity work (NICE (2013). For the interviews, we developed a protocol to guide discussion in focus groups. This protocol incorporated general topics identified in the taxonomy to allow participants to openly discuss their experiences in cybersecurity MTSs (e.g., "Can you walk me through what happens when a potential incident is detected?"). All focus groups were recorded and transcribed by a professional transcription service. Then, each transcript was divided into codeable units. These units were then coded by four coders working in pairs based on an outline version of the taxonomy wherein the coders identified whether the codeable unit represented a task statement categorized a) at the individual, within team, or multiteam system level, b) as a process, behavior, or outcome, and c) as reactive or proactive. After training, agreement between coders reached 90% or above.

After some initial interviews, the first frequency counts were tabulated based on the taxonomy coding of NICE statements and statements transcribed from four focus groups. These counts reflected the number of references to a particular taxon. Subsequent focus groups and interviews were used to refine the taxonomy until it contained 69 total validated taxa (see Zaccaro, et al., 2016, for additional details).

A review of the frequency counts led to one of three outcomes: 1) the tasks and subtasks were validated, 2) the subtasks that were not validated were not substantially different from other validated subtasks, or 3) the validation of some subtasks implied the validation of related subtasks that were currently not validated. In order to determine whether non-validated subtasks fell under category 2 or 3, project subject matter experts (SMEs) decided whether these subtasks should be removed or validated by proxy. In addition to the three categories described above, some task were not represented at the task or subtask level. In this case, the recommended action was to focus on these particular categories in subsequent interviews/focus groups, and ultimately, to consider deletion of these taxa if future focus groups failed to validate them. The result of these efforts are shown later in this appendix.

A.4 How CSIRT Managers Can Use the Performance Taxonomy

The performance taxonomy can be used by CSIRT managers to inform hiring, training, performance management, and CSIRT process models. The taxonomy can help managers connect the entire process of hiring, evaluating, and training employees by using very specific descriptions of the behaviors that the job requires to provide clarity and help employees understand exactly what the job entails. The specific ways that the taxonomy can inform hiring, evaluating, and training of CSIRT employees are described below.

A.4.1 PREPARING POSITION DESCRIPTIONS

When selecting job applicants, using a job description that accurately describes the performance requirements of the job will enable hiring managers to more easily compare applicants' skills and experiences to the specific tasks required by the job. Such an accurate job description also helps applicants compare their own skill set to the description to determine whether they will be a good fit for the job. As an example, when CSIRT managers are hiring for a position that involves *watching and identifying potential security incidents*, they can use that section of the taxonomy that describes the tasks involved with identifying security vulnerabilities in the position description:

- "Scan and monitor information systems for emerging trends as well as potential weaknesses, deteriorations, and obsolescence;"
- "Identify emerging security vulnerabilities and possible threats."

Linking the performance requirements in the validated taxonomy to the language in a position description will help both applicants and hiring managers in the screening process, leading to a more efficient process for classifying, reviewing, and selecting applicants. Overall, this process should lead to better CSIRT performance when the people who are the best fit for the job apply and are selected.

A.4.2 DEVELOPING PERFORMANCE EVALUATION AND MANAGEMENT TOOLS

In order to use the taxonomy to inform CSIRT performance management and evaluation, CSIRT managers can look at the behaviors outlined in the taxonomy and select the ones that are most important for performance in their particular contexts. These selected items should then be used to populate a performance evaluation instrument. For example, when creating a performance evaluation plan for a watch team or a network monitoring position, managers can include the following items on subsequent performance evaluations and then evaluate how well analysts complete each task:

- Attend to intrusion detection alerts
- Gather additional information about nature of attack
- Assess for false positives
- Select cases for triage and further response
- Send out initial incident alerts
- Prepare a ticket for the incident

Such specific item-level evaluations can promote more effective performance feedback. Managers can also use these statements at the team and multiteam system level to a) gain an understanding of the types of processes that require coordination between team members and members of different teams and b) evaluate the effectiveness of these processes. Based on managers' evaluations, steps can be taken to improve performance in specific areas and at specific levels.

A.5 Designing Training Programs

The taxonomy provides a clear set of behaviors required for effective CSIRT performance. Once CSIRT managers identify areas for development through the performance evaluation and management process, they can tailor a training or development program, including learning objectives, instructional design, and training evaluation, to address these specific gaps. For example, if an employee's performance evaluation reveals that he or she needs development or training in the area of *identifying emerging security vulnerabilities and possible threats*, a manager can identify specific learning objectives reflecting this training need, and include them as part of the employee's individualized development plan.

The hiring manager can also use the taxonomy to plan training for the entire cybersecurity team or MTS. In such instances, the manager would focus on behaviors at the "Team" or "Multiteam System" levels in the taxonomy. For example, if a performance evaluation based on the team level tasks in the taxonomy reveals that the team needs training to better "reach consensus on a shared understanding of the veracity and probability of potential vulnerabilities and threats," then the manager sets team instructional learning objectives for a training simulation that specifically targets this behavior. Appendix D provides examples of training programs of instruction.

A.6 Informing CSIRT Process Models

CSIRT Process Models are a mapping of how incident management occurs in CSIRTs (Alberts, Dorofee, Kilcrece, Ruefle, & Zajicek, 2004; Maj, Reijers, & Stikvoort, 2010). They typically take the form of a workflow diagram that shows details such as the tasks required for a CSIRT to be successful, the goals and objectives of the CSIRT, the roles and responsibilities of the people in the CSIRT, and the order in which tasks are completed. The performance taxonomy can inform the development of CSIRT process models by providing a set of behaviors that must occur at the individual, team, and multiteam system levels to accomplish the tasks in the process model.   The tasks and subtasks listed under performance processes (planning) and performance behaviors (outcomes) provide a basis for specifying in greater detail than current process models the steps analysts need to initiate to accomplish particular performance tasks.

References

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams–Challenges in supporting the organisational security function. *Computers & Security, 31(5)*, 643-652.

Alberts, C., Dorofee, A., Killcrece, G., Rue e, R., & Zajicek, M. (2004). Defining incident management processes for CSIRTs: A work in progress (No. CMU/SEI-2004-TR-015). Software Engineering Institute, Carnegie Mellon University. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a453378.pdf

Borman, W. C., Ackerman, L. D., Kubisiak, U. C., & Quigley, A. M. (1994). Development of a performance rating program in support of Department of Labor test validation research. *Contract, (93-2)*, 93-3.

Borman, W. C., & Brush, D. H. (1993). More progress toward a taxonomy of managerial performance requirements. *Human performance, 6(1)*, 1-21.

Borman, W. C., Bryant, R. H., & Dorio, J. (2010). The measurement of task performance as criteria in selection research. Handbook of employee selection. New York: Psychology Press.

Brownlee, N., & Guttman, E. (1998). RFC2350: Expectations for computer security incident response. Internet RFCs.

Campbell, J. P., McCloy, R. A., Oppler, S. H., & Sager, C. E. (1993). A theory of performance. Personnel selection in organizations, 3570.

ENISA. (2010). Good practice guide for incident management. Retrieved from https://www.enisa.europa.eu/activities/cert/support/incident-management.

Fleishman, E. A., & Zaccaro, S. J. (1992). Taxonomic classifications of team tasks. In R. W. Swezey & E. Salas (Ed.), *Teams: Their training and performance* (pp. 31-56). Norwood, NJ: ABLEX.

Hunt, S. T. (1996). Generic work behavior: An investigation into the dimensions of entry-level, hourly job performance. *Personnel Psychology, 49(1)*, 51-83.

Kozlowski, S. W. J., & Ilgen, D. R. (2006). Enhancing the effectiveness of work groups and teams. *Psychological Science in the Public Interest, 7, 77–124*. doi: 10.1111/j.1529-1006.2006.00030.x

Maj, M., Reijers, R., & Stikvoort, D. (2010). European Network and Information Security Agency (ENISA) Good practice guide for incident management. Retrieved from https://www.enisa.europa.eu/activities/cert/support/incident-management.

Mathieu, M., Marks, M. A., & Zaccaro, S. J. (2001). Multi-team systems theory. In N. Anderson, D. Oniz, & C. Viswesvaran (Eds.), *The International Handbook of Work and Organizational Psychology (pp. 289-312)*. London: Sage Publications.

NICE. (2013). The national cybersecurity workforce framework 1.0. Retrieved from http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_interactive.pdf

Peterson, N. G., Mumford, M. D., Borman, W. C., Jeanneret, P., & Fleishman, E. A. (1999). An occupational information system for the 21st century: The development of O* NET. American Psychological Association.

Ruefle, R. (2007). Defining computer security incident response teams.

Salas, E., Dickinson, T. L., Converse, S. A., & Tannenbaum, S. I. (1992). Toward an understanding of team performance and training.

Sundstrom, E., DeMeuse, K. P., & Futrell, D. (1990). Work teams: Applications and effectiveness. *American Psychologist, 45*, 120-133

Viswesvaran, C. (1993). Modeling job performance: Is there a general factor?. Iowa Univ iowa City.

Wildman, J. L., Bedwell, W. L., Salas, E., & Smith-Jentsch, K. A. (2011). Performance measurement at work: A multilevel perspective.

Zaccaro, S.J., Hargrove, A.C., Chen, T.R., Repchick, K.M., and McCauseland, T. (2016) A comprehensive multilevel taxonomy of cybersecurity incident response performance. In S. J. Zaccaro, R. S. Dalal, L.E. Tetrick, & J.A. Steinke, (Eds.), *The Psychosocial dynamics of cyber security (13-55)*. New York: Taylor & Francis.

PROACTIVE PERFORMANCE – INDIVIDUAL LEVEL OF ANALYSIS			
	PERFORMANCE PROCESSES (PLANNING)	PERFORMANCE BEHAVIORS (EXECUTION)	PERFORMANCE OUTCOMES (EFFECTIVENESS)
	A. Define mission, tasks, and services i. Identify CSIRT mission scope and requirements, ii. Identify corresponding incident response tasks, iii. Identify environmental conditions, practical constraints, iv. Identify necessary resources	B. Formalize the mission, tasks, and services i. Consult with relevant stakeholders about mission parameters and stakeholder requirements ii. Obtain management support and appropriate funding to carry out mission and services iii. Establish and communicate formal mission and task statements	C. Task effectiveness i. Solution quality 1. Comprehensiveness 2. Innovation ii. Quantity iii. Efficiency vi. Secure configuration v. Vulnerability reduction D. Cognitive outcomes i. Customer 1. Knowledge and skill acquisition ii. Component team member 2. Knowledge and skill acquisition E. Affective outcomes i. Customer 1. Satisfaction with component team member 2. Commitment to component team member ii. Component team member 1. Job satisfaction 2. Commitment a. Component team b. Other component teams c. Cyber security multiteam system d. Organization e. Constituency F. Motivational outcomes i. Customer 1. Task Efficacy ii. Component team member 2. Task Efficacy G. Well-being outcomes i. Customer 1. Psychological 2. Physical ii. Component team member 1. Psychological 2. Physical H. Turnover
	I. Determine necessary security tools, applications, and infrastructure for establishing the CSIRT i. Identify and specify cybersecurity infrastructure requirements ii. Generate potential tools, programs, protocols, and methods that meet infrastructure requirements iii. Evaluate and select security enhancement interventions that provide best fit to infrastructure requirements iv. Plan implementation of selected security measures tools, and applications	J. Implement selected CSIRT security tools, applications, and infrastructure for CSIRT set-up	
	K. Design procedures for maintenance of security tools, applications, and infrastructure	L. Execute maintenance procedures for security tools, applications, and infrastructure i. Implement scheduled maintenance activities ii. Monitor operating conditions of existing security tools, applications, and infrastructure	
	M. Identify potential security vulnerabilities and possible threats i. Scan, monitor and test information systems for potential weaknesses, deteriorations, and obsolescence ii. Identify emerging security vulnerabilities and possible threats iii. Forecast criticality of potential vulnerabilities and potential threats	N. Post/publicize information about potential threats and system weaknesses, deteriorations, and obsolescence	
	O. Identify proactive security tools, applications, , and solutions i. Generate and evaluate technological solutions for potential and emerging threats ii. Assess and develop system capabilities to integrate potential solutions iii. Develop plans for implementing proactive technological solutions	P. Implement proactive safeguards and solutions i. Implement and update necessary infrastructure changes, software revisions, and new applications ii. Inform cyber security personnel and constituencies of infrastructure changes and of the use of new software and proactive security applications	

PROACTIVE PERFORMANCE – WITHIN COMPONENT TEAMS LEVEL OF ANALYSIS

	PERFORMANCE PROCESSES (PLANNING)	PERFORMANCE BEHAVIORS (EXECUTION)	PERFORMANCE OUTCOMES (EFFECTIVENESS)
	A. Define mission, tasks, and services i. Exchange and evaluate ideas about CSIRT mission priorities and requirements ii. Develop a shared understanding of the CSIRT's mission iii. Determine CSIRT strategies and interaction procedures to best accomplish mission goals and priorities	B. Formalize mission, tasks, and services i. Implement CSIRT interaction protocols to coordinate team members' actions around mission accomplishment	C. Task effectiveness i. Solution quality 1. Comprehensiveness 2. Innovation ii. Secure configuration iii. Vulnerability reduction vi. Quantity v. Efficiency 1. Component team infrastructure efficiency 2. Component team cost-benefit efficiency D. Cognitive outcomes i. Customer 1. Knowledge and skill acquisition ii. Component teams 1. Knowledge and skill acquisition 2. Shared mental model 3. Transactive memory system E. Affective outcomes i. Customer 1. Satisfaction component team 2. Commitment to component team ii. Component team 1. Trust 2. Psychological safety 3. Viability 4. Satisfaction F. Motivational outcomes i. Customer 1. Task Efficacy ii. Component team 1. Collective efficacy 2. Cohesion a. Task b. Interpersonal G. Organizational reputation i. Reports from the media
	H. Determine necessary security tools, applications, and infrastructure for establishing the CSIRT i. Exchange relevant information and ideas among team members about cybersecurity infrastructure requirements ii. Generate and evaluate members' ideas and proposals about potential security measures, tools, and applications that meet infrastructure requirements iii. Garner collective endorsement for the most appropriate security measures tools, and applications iv. Plan team implementation of selected security measures tools, and applications	I. Implement security tools, applications, and infrastructure for CSIRT set-up i. Coordinate members' implementation of selected security measures, tools, and applications ii. Engage in collective monitoring and back-up behavior of team members during implementation of security measures, tools, and applications	
	J. Design team level procedures for maintenance of security tools, applications, and infrastructure i. Exchange relevant information among team members on necessary maintenance procedures and standards ii. Share information with team members about operating conditions of existing security tools, applications, and infrastructure	K. Execute procedures for maintenance of security tools, applications, and infrastructure i. Assign team member roles in infrastructure maintenance functions. ii. Coordinate and balance team member activities to accomplish maintenance procedures	
	L. Identify potential security vulnerabilities and threats to cybersecurity infrastructure and information systems i. Exchange information and ideas with team members about emerging security trends as well as potential infrastructure weaknesses, deteriorations, and obsolescence ii. Reach consensus on the veracity and probability of potential vulnerabilities and threats to cybersecurity infrastructure	M. Test for potential security vulnerabilities and threats i. Coordinate member actions in conducting multiple and different tests of existing cybersecurity infrastructure and information systems for potential weaknesses, deteriorations, and obsolescence ii. Exchange data and reach consensus on information to be posted/publicized about potential threats and system weaknesses, deteriorations, and obsolescence	
	N. Identify proactive security tools, applications, and solutions. i. Exchange information and ideas among team members about software, tools, and other technological solutions for potential and emerging threats ii. Exchange information and expertise about system capabilities relative to candidate solutions iii. Reach consensus and select the best-fitting software, tools, and other solutions for potential and emerging threats iv. Develop plans for implementation of selected solutions	O. Implement proactive security tools, applications and solutions i. Assign member roles for implementation processes ii. Coordinate and balance team member activities to implement necessary infrastructure programming, software revisions, and new applications	

PROACTIVE PERFORMANCE – WITHIN COMPONENT TEAMS LEVEL OF ANALYSIS (CONT.)

	PERFORMANCE PROCESSES (PLANNING)	PERFORMANCE BEHAVIORS (EXECUTION)	PERFORMANCE OUTCOMES (EFFECTIVENESS)
	P. Plan team system structures i. Identify general team member roles and role requirements ii. Define team norms iii. Determine team reward structure iv. Determine within-team performance criteria and feedback structures	Q. Implement component team structure i. Staff the team to match role requirements ii. Train team members to match role requirements iii. Foster acceptance of team norms iv. Implement and enforce team standards v. Implement and enforce team reward structure vi. Facilitate team confidence, motivation, and task-based cohesion	

PROACTIVE PERFORMANCE – BETWEEN COMPONENT TEAMS LEVEL OF ANALYSIS

PERFORMANCE PROCESSES (PLANNING)	PERFORMANCE BEHAVIORS (EXECUTION)	PERFORMANCE OUTCOMES (EFFECTIVENESS)
A. Define mission, tasks, and services i. Exchange and evaluate CSIRT multiteam mission priorities and requirements from different component teams ii. Reach a consensus among component teams of the overall incident response mission priorities and requirements iii. Determine CSIRT multiteam strategies and interaction procedures and strategies to accomplish mission goals and priorities	B. Formalize mission, tasks, and services i. Implement CSIRT between-team interaction protocols to coordinate component teams' actions around CSIRT multiteam system mission accomplishment	C. Task effectiveness i. Solution quality 1. Comprehensiveness 2. Innovation ii. Secure configuration iii. Vulnerability reduction vi. Quantity v. Efficiency 1. Cyber security multiteam system infrastructure efficiency 2. Cyber security multiteam system cost-benefit efficiency D. Cognitive outcomes i. Customer 1. Knowledge and skill acquisition ii. Between component 1. Knowledge and skill acquisition 2. Shared mental model 3. Transactive memory system E. Affective outcomes i. Customer 1. Satisfaction with cyber security multiteam system 2. Commitment to cyber security multiteam system ii. Between component team 1. Trust 2. Psychological safety 3. Viability 4. Satisfaction F. Motivational outcomes i. Customer 1. Task Efficacy ii. Between component teams 1. Collective efficacy 2. Cohesion a. Task b. Interpersonal G. Organizational reputation i. Reports from the media
H. Determine necessary security tools, applications, and infrastructure for establishing the CSIRT multiteam system i. Exchange relevant information and ideas among component teams about cybersecurity infrastructure requirements ii. Generate and evaluate members' ideas and proposals about potential security measures, tools, and applications that meet infrastructure requirements iii. Garner collective endorsement for the most appropriate security measures tools, and applications iv. Plan between-team implementation of selected security measures, tools, and applications	I. Implement security tools, applications, and infrastructure i. Coordinate component teams' implementation of security measures, tools, and applications ii. Engage in collective monitoring and back-up behavior of component teams during implementation of security measures, tools, and applications	
J. Design multiteam system level procedures for maintenance of security tools, applications, and infrastructure i. Exchange relevant information between component teams on necessary maintenance requirements and standards ii. Integrate the maintenance requirements for the security tools, applications, and infrastructure of different component teams iii. Share information with component teams about operating conditions of existing security tools, applications, and infrastructure	K. Execute procedures for maintenance of security tools, applications, and infrastructure i. Assign component team roles in infrastructure maintenance functions ii. Coordinate and balance component team activities to accomplish infrastructure maintenance procedures	
L. Identify potential security vulnerabilities and threats to cybersecurity infrastructure and information systems i. Exchange information and ideas across component teams about emerging security trends and specific threats ii. Exchange information across component teams about potential infrastructure weaknesses, deteriorations, and obsolescence iii. Reach consensus across component teams on the veracity and probability of potential vulnerabilities and threats to cybersecurity infrastructure	M. Test for potential security vulnerabilities and threats i. Coordinate actions of component teams in conducting multiple and different tests of existing cybersecurity infrastructure and information systems for potential weaknesses, deteriorations, and obsolescence ii. Exchange data and reach consensus across component teams on information to be posted/publicized about potential threats and system weaknesses, deteriorations and obsolescence	

PROACTIVE PERFORMANCE – BETWEEN COMPONENT TEAMS LEVEL OF ANALYSIS (CONT.)

	PERFORMANCE PROCESSES (PLANNING)	PERFORMANCE BEHAVIORS (EXECUTION)	PERFORMANCE OUTCOMES (EFFECTIVENESS)
	N. Identify proactive security tools, applications, and solutions i. Exchange information and ideas among component teams about how new software, tools, and other technological solutions for potential and emerging threats ii. Exchange information and expertise across component teams about system capabilities relative to candidate solutions iii. Reach consensus across component teams and select the best-fitting software, tools, and other solutions for potential and emerging threats iv. Develop plans for implementation across component teams of selected solutions	O. Implement proactive security tools, applications, and solutions i. Assign component team roles for implementation processes ii. Coordinate and balance component team activities to implement necessary infrastructure programming, software revisions, and new applications ats	
	P. Plan multiteam system structures i. Identify component teams that need to work together within an MTS ii. Define general component team roles and proximal goals/tasks iii. Define MTS norms iv. Determine MTS reward structures v. Determine MTS-level performance criteria and feedback structures	Q. Establish multiteam system structures i. Staff the CSIRT-MTS with selected component teams to match role requirements ii. Train component teams to match role requirements iii. Foster acceptance of MTS norms iv. Implement MTS reward structures v. Facilitate between-team and MTS confidence, motivation, and task-based cohesion	

REACTIVE PERFORMANCE – INDIVIDUAL LEVEL OF ANALYSIS

	PERFORMANCE PROCESSES (PLANNING)	PERFORMANCE BEHAVIORS (EXECUTION)	PERFORMANCE OUTCOMES (EFFECTIVENESS)
	A. Detect and gather information about security incident(s) i. Monitor systems and attend to intrusion detection alerts ii. Gather additional information about nature of potential events iii. Assess event data for false positives iv. Select cases for triage and further incident response	B. Alert others about security incident(s) i. Send out initial incident alerts ii. Prepare a ticket for the incident	C. Task effectiveness i. Solution quality 1. Comprehensiveness 2. Innovation ii. Incident Handling Capability iii. Recovery Capability iv. Quantity v. Efficiency D. Cognitive outcomes i. Customer 1. Knowledge and skill acquisition ii. Component team member 2. Knowledge and skill acquisition E. Affective outcomes i. Customer 1. Satisfaction with component team member 2. Commitment to component team member ii. Component team member 1. Job satisfaction 2. Commitment a. Component team b. Other component teams c. Cyber security multiteam system d. Organization e. Constituency F. Motivational outcomes i. Customer 1. Task Efficacy ii. Component team member 2. Task Efficacy G. Well-being outcomes i. Customer 1. Psychological 2. Physical ii. Component team member 1. Psychological 2. Physical H. Turnover
	I. Triage incoming incident(s) i. Assess and categorize identified incidents (new/old; level of typicality, level of potential harm, etc.) ii. Define and prioritize problems caused by the incident	C. Communicate triage assessment i. Update case file based on assessment, prioritization and categorization ii. Communicate with other responders or affected constituencies when incident is determined to reach level of immediate notification	
	J. Analyze incident(s) i. Forecast potential damage from incident ii. Identify constituents affected by incident iii. Gather and examine evidence and artifacts related to the incident iv. Determine the incident cause	D. Communicate and act on incident analysis i. Prepare analysis report ii. Handoff and/or escalate incident to other responders as needed	
	K. Develop comprehensive incident remediation solution i. Define specifications of potential best-fitting solutions ii. Generate and research potential solutions that match desired specifications iii. Simulate potential best-fitting solutions iv. Select best-fitting solution v. Develop incident remediation solution implementation plan	L. Implement incident remediation solution i. Execute selected security tools, applications, and/or procedures to resolve incident ii. Monitor functioning of implemented security tools, applications, and/or procedures to confirm incident resolution	
		M. Document and report action logs i. Complete and file written analysis and summary of incident handling case (i.e., close ticket) ii. Post related incident handling information and new threat information to internal communication sites (e.g., wiki, blog, etc.)	
	N. Conduct after-action review i. Gather information and evaluate the effectiveness of completed incident handling cases for lessons learned ii. Assess and evaluate necessary revisions to existing cybersecurity policies, procedures, tools, applications and/or infrastructure iii. Develop implementation plan for necessary revisions to existing cybersecurity policies, procedures, tools, applications and/or infrastructure	O. Implement necessary after-action adaptation i. Implement necessary changes to existing incident handling policies, procedures, tools, applications and/or infrastructure ii. Monitor functioning of implemented changes to existing incident handling policies, procedures, tools, applications and/or infrastructure to ensure greater adaptation	

REACTIVE PERFORMANCE – WITHIN TEAMS LEVEL OF ANALYSIS

	PERFORMANCE PROCESSES (PLANNING)	PERFORMANCE BEHAVIORS (EXECUTION)	PERFORMANCE OUTCOMES (EFFECTIVENESS)
	A. Detect and gather information about security incident(s) i. Exchange information and ideas with other team members about nature of attack ii. Gather evaluations and concurrence from other team members on assessments of false positives iii. Reach consensus on cases to be selected for triage and further incident response	B. Alert others about security incident(s) i. Coordinate team members' activities in the distribution of initial alerts	C. Task effectiveness i. Solution quality 1. Comprehensiveness 2. Innovation ii. Incident Handling Capability Data iii. Recovery Capability vi. Quantity v. Efficiency 1. Component team infrastructure efficiency 2. Component team cost-benefit efficiency D. Cognitive outcomes i. Customer 1. Knowledge and skill acquisition ii. Component 1. Knowledge and skill acquisition 2. Shared mental model 3. Transactive memory system E. Affective outcomes i. Customer 1. Satisfaction with component team 2. Commitment to a component team ii. Component team 1. Collective efficacy 2. Trust 3. Psychological safety 4. Viability 5. Satisfaction F. Motivational outcomes i. Customer 1. Task Efficacy ii. Component team 1. Collective efficacy 2. Cohesion a. Task b. Interpersonal G. Organizational reputation i. Reports from the media
	H. Triage (assess, categorize, and prioritize) incoming incident(s) i. Share assessments of identified threats ii. Exchange information and reach agreement about how to categorize identified incidents (new/old; recognize typicality, level of potential harm, etc.) within team iii. Exchange information and reach agreement about the problems caused by incidents, and their prioritization	I. Communicate triage assessment i. Coordinate on updating of case file (i.e., ticket) ii. Collaborate on when and how to communicate with other responders or affected constituencies	
	J. Analyze incident(s) i. Exchange relevant information within the team to forecast potential incident damage ii. Exchange relevant information within the team to identify constituents affected by incident iii. Exchange evidence and artifacts related to the incident. iv. Reach consensus within the team on the cause of the incident	K. Communicate and act on incident analysis i. Coordinate team member activities for creation and communication of incident analysis report ii. Collaborate on handoff and/or escalation of incident to other responders, as needed	
	L. Develop comprehensive incident remediation solution i. Exchange information among team members and collaborate on specifications for potential best-fitting solutions; ii. Reach consensus on desired solution specifications iii. Exchange ideas about potential solutions; iv. Exchange information about members' expertise and experiences with potential solutions v. Conduct team-wide simulation of potential best-fitting solutions vi. Reach team consensus on best-fitting solutions vii.Determine team members' roles in solution implementation plans	M. Implement incident remediation solution i. Coordinate team members' actions in executing selected security solution ii. Assign team members different roles in monitoring functioning of implemented security solution	
		N. Document and report action logs i. Integrate contributions from participating team members into case summary ii. Coordinate members contributions to the posting of case information to internal communication sites (e.g., wikis, blogs)	

REACTIVE PERFORMANCE – WITHIN TEAMS LEVEL OF ANALYSIS (CONTINUED)			
	PERFORMANCE PROCESSES (PLANNING)	PERFORMANCE BEHAVIORS (EXECUTION)	PERFORMANCE OUTCOMES (EFFECTIVENESS)
	O. Conduct team after-action reviews i. Exchange information and evaluate the effectiveness of team interactions and collective activities during all phases of completed incident handling cases ii. Assess and evaluate necessary revisions to existing team cybersecurity policies, interaction protocols and member roles iii. Develop implementation plan for necessary revisions to existing team cybersecurity policies, procedures, tools, applications and/or infrastructure	P. Implement necessary after-action adaptation i. Assign member roles in implementation of necessary changes to existing incident handling policies, procedures, tools, applications and/or infrastructure ii. Coordinate members activities in implementation of necessary changes to existing incident handling policies, procedures, tools, applications and/or infrastructure iii. Coordinate of monitoring of implemented changes across team members to ensure greater adaptation	
		Q. Manage interpersonal component team members' interactions i. Monitor and facilitate team communication protocols ii. Manage conflict among team members iii. Monitor and maintain cohesion among team members iv. Address morale issues arising among team members	

REACTIVE PERFORMANCE – BETWEEN TEAMS LEVEL OF ANALYSIS

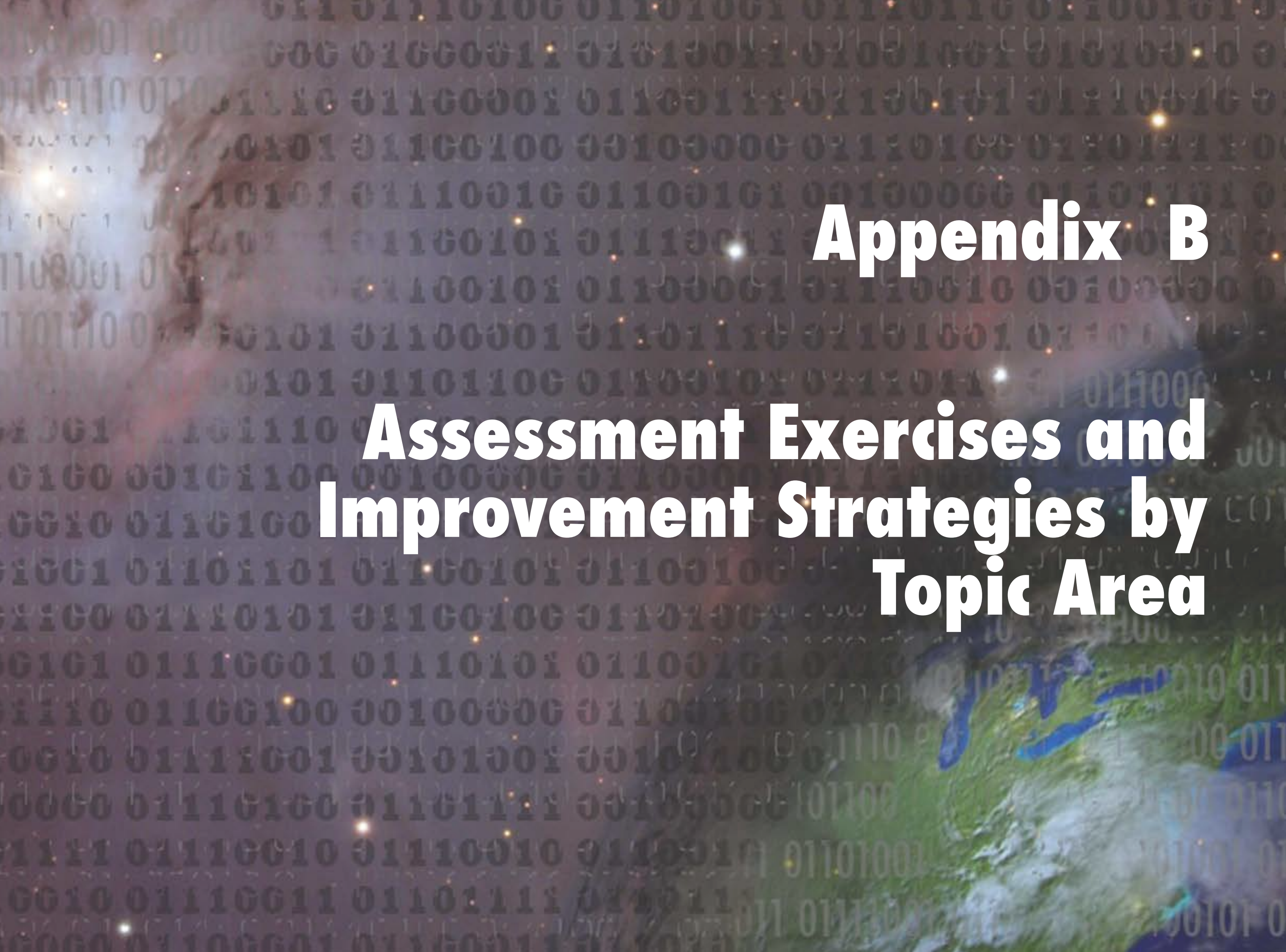
	PERFORMANCE PROCESSES (PLANNING)	PERFORMANCE BEHAVIORS (EXECUTION)	PERFORMANCE OUTCOMES (EFFECTIVENESS)
	A. Detect and gather information about security incident(s) i. Coordinate and consult with possibly affected component teams to gather and exchange information about the nature of the attack ii. Gather evaluations and concurrence from appropriate component teams on assessments of false positives iii. Reach consensus across relevant component teams on cases to be selected for triage and further incident response	B. Alert others about security incident(s) i. Coordinate component teams roles in distribution of initial alerts to their respective constituencies and potentially affected clients outside of the MTS	C. Task effectiveness i. Solution quality 1. Comprehensiveness 2. Innovation ii. Incident Handling Capability Data iii. Recovery Capability vi. Quantity v. Efficiency 1. Cyber security multiteam system infrastructure 2. Cyber security multiteam system cost-benefit D. Cognitive outcomes i. Customer 1. Knowledge and skill acquisition ii. Between component 1. Knowledge and skill acquisition 2. Shared mental model 3. Transactive memory system E. Affective outcomes i. Customer 1. Satisfaction with cyber security multiteam system 2. Commitment to cyber security multiteam system ii. Between component team 1. Trust 2. Psychological safety 3. Viability 4. Satisfaction F. Motivational outcomes i. Customer 1. Collective Efficacy 2. Task Efficacy ii. Between component teams 1. Cohesion a. Task b. Interpersonal G. Organizational reputation i. Reports from the media
	H. Triage (assess, categorize, and prioritize) incoming incident(s) i. Share assessments of identified threats across relevant component teams ii. Exchange information and reach agreement across affected component teams about how to categorize identified incidents (new/old; recognize typicality, level of potential harm, etc.) iii. Exchange information and reach agreement across affected component teams about the problems caused by incidents, and their prioritization	I. Communicate Assessments i. Coordinate across component teams on updating of case files ii. Collaborate across component teams on when and how to communicate with other responders or affected constituencies	
	J. Analyze incident(s) i. Exchange relevant information across component teams to forecast potential incident damage ii. Exchange relevant information across component to identify constituents affected by incident iii. Exchange evidence and artifacts related to the incident across multiple component teams iv. Reach consensus across component teams on the cause of the incident	K. Analytical behaviors i. Collaborate with component teams to creation and communication of analysis report ii. Collaborate with other component teams on handoff and/or escalation of incident to other responders	
	L. Develop comprehensive incident remediation solutions i. Exchange information among component teams on specifications for potential solutions ii. Reach consensus across component teams on desired solution specifications iii. Exchange ideas among component teams about potential solutions iv. Exchange information about component teams functions, expertise, and experiences with potential solutions v. Conduct simulation with multiple component teams of potential best fitting solutions vi. Reach consensus among multiple component teams about best-fitting solutions vii.Determine roles of each component team in solution implementation plans	M. Implement selected incident remediation solution(s) i. Coordinate across component teams in executing selected security solutions ii. Assign component teams different roles in monitoring functioning of implemented incident resolution solutions	

REACTIVE PERFORMANCE – BETWEEN TEAMS LEVEL OF ANALYSIS (CONTINUED)

	PERFORMANCE PROCESSES (PLANNING)	PERFORMANCE BEHAVIORS (EXECUTION)	PERFORMANCE OUTCOMES (EFFECTIVENESS)
		N. Document and report action logs i. Integrate contributions from participating component teams into case summary ii. Coordinate component team contributions to the posting of case information to internal communication sites	
	O. Conduct after-action review i. Exchange information and evaluate the effectiveness of interactions and activities across all component teams involved in incident handling cases ii. Assess and evaluate necessary revisions to existing MTS cybersecurity policies, interaction protocols, and component team roles iii. Develop implementation plans fo necessary revisions to existing MTS cybersecurity policies, interaction protocols, and component team roles	P. Implement after action adaptation strategies i. Assign component team roles in implementation of necessary changes to existing incident handling policies, procedures, tools, applications and/or infrastructure ii. Coordinate component team activities in implementation of necessary changes to existing incident handling policies, procedures, tools, applications and/or infrastructure iii. Coordinate of monitoring of implemented changes across component teams to ensure greater adaptation	
		O. Manage interpersonal component team interactions i. Monitor and facilitate communication protocols and interactions among component teams ii. Manage conflicts among component teams iii. Monitor and maintain cohesion between component team members, and across the incident response MTS iv. Address morale issues between component team members, and across the incident response MTS	

Appendix B

Assessment Exercises and Improvement Strategies by Topic Area



Contents

B.1 Assessment Exercises and Improvement Strategies by Topic Area

Consider these statements to determine the improvement strategies that would most benefit your CSIRT.

★ *Strategies denoted with a star are highly recommended

CHAPTER 3: MEASURING AND EVALUATING CSIRT PERFORMANCE

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. I consider not only conventional, objectively-derived performance metrics, but also subjectively-derived (e.g., using ratings) performance metrics..
2. I consider not only the quantity of performance, but also the quality of performance.
3. I consider not only how well an analyst performs under normal operating circumstances (i.e.,“typical” performance), but also how he or she performs when confronted with very serious incidents (i.e.,“maximum” performance).
4. I consider not only performance after an incident is detected (i.e., reactive performance), but also performance that occurs before an incident is detected (i.e., proactive performance).
5. I consider not only performance at the individual level, but also performance at the team level or other levels (performance at the broader multiteam system level).
6. I consider not only conventional performance outcomes, but also psychological (e.g., well-being) outcomes.

IMPROVEMENT STRATEGIES

Strategy 1: Balance Measuring Quantity and Quality

Strategy 2: Measure Maximum Performance in Addition to Typical Performance

Strategy 3: Measure Both Proactive and Reactive Performance

Strategy 4: Determine the Appropriate Level of Measurement

★ Strategy 5: Create a Balanced Scorecard of Performance Measurement

CHAPTER 4: DECISION-MAKING IN CSIRTS

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. Analyst expertise is considered explicitly when analysts are assigned (or assign themselves) to incidents.
2. Incident severity is considered explicitly when analysts are assigned (or assign themselves) to incidents.
3. Decision-making skills are emphasized in analyst training activities.
4. My analysts consider all necessary information before they make decisions in response to an incident.
5. My analysts comprehensively rehearse their response plans (including mentally testing them for ways in which they could go wrong) before implementing them.
6. When hiring new analysts, decision-making skills are emphasized.
7. My analysts decide correctly that they should include other analysts in their incident mitigation efforts.
8. Members on my team are proactive, soliciting help from team members.
9. My team solicits help proactively from other teams in the CSIRT MTS.
10. My team asks other teams in the CSIRT MTS to help them resolve an incident when such help is necessary.
11. My team takes the initiative when deciding to include other teams in a CSIRT MTS in their incident mitigation efforts.

IMPROVEMENT STRATEGIES

Strategy 1: Selecting for Decision-Making Skills

Strategy 2: Training Decision-Making Skills

Strategy 3: Cognitive Prompts to Reduce Overconfidence and Confirmation Bias

★ Strategy 4: Using Mnemonics to Capture Necessary Information

★ Strategy 5: Using Adaptive Case Management

CHAPTER 5: COMMUNICATION EFFECTIVENESS IN INCIDENT RESPONSE

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. Messages sent among my team members contain all critical information.
2. Messages sent or received by the team are understood clearly.
3. My team members ask for clarification for messages received from others when they are unsure of something.
4. My team members confirm receipt and understanding of critical communications.
5. Information is received on time when trying to address a cyber threat.
6. Messages are sent to the correct recipient during different phases of incident resolution.
7. Complete and accurate information is passed during handoffs between different individuals in my team.
8. My team members quickly resolve communication issues with individuals on their teams.
9. My team members quickly resolve communication issues with team members from other cultures.
10. Messages sent between teams in the CSIRT MTS contain all critical information.
11. Different teams ask for clarification for messages received from other teams when they are unsure of something.
12. Confirmation of receipt and understanding of critical communications occurs between teams.
13. Complete and accurate information is passed during handoffs between different teams.
14. Teams quickly resolve communication issues with other teams.
15. Teams in the CSIRT MTS designate a point person to communicate with other teams or external parties.

IMPROVEMENT STRATEGIES

★ Strategy 1: Communication Charters

★ Strategy 2: Handoff Checklists

★ Strategy 3a: Scenario-based Practice with Pre-briefing

★ Strategy 3b: Team Simulation Training

Strategy 4a: Virtual Displays

Strategy 4b: Wiki Best Practices

Strategy 5: Boundary-spanner Designation

Strategy 6: Work Space Design

Strategy 7: Situational Interviews to Select People Communication Skills

CHAPTER 7: COLLABORATIVE PROBLEM-SOLVING IN INCIDENT RESPONSE

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. Team members in my CSIRT solicit help from each other proactively.
2. My team members get together to brainstorm and to consult each other about incident resolution.
3. My team members use the knowledge they have gained from other team members in resolving a novel incident.
4. My team members work together to determine the potential consequences of an event or threat to the cybersecurity of the organization or to constituents.
5. Members of my CSIRT consider multiple viewpoints when resolving an incident.
6. Members of my CSIRT are willing to switch to new kinds of solutions when existing ones may not be the best.
7. Members of my CSIRT try new ways of thinking about novel events and incidents.
8. Members of my CSIRT adopt new ways of resolving incidents.
9. Members of my CSIRT are comfortable deviating from normal or typical ways of resolving incidents.
10. My team members change their behaviors or protocols as a result of previous incidents.
11. Members of my team are likely to try new ideas and solutions when resolving incidents.
12. My team members incorporate the expertise of other teams into incident resolution.
13. Teams in my CSIRT MTS solicit help from other teams proactively.
14. Multiple teams get together to brainstorm and to consult each other about incident resolution.
15. Multiple teams work together to determine the potential consequences of an event or threat to the cybersecurity of the organization or to constituents.
16. Teams in the CSIRT MTS change their ways of interacting with one another as a result of previous incidents.

IMPROVEMENT STRATEGIES

★ Strategy 1: Engage in pre-mission planning (or pre-briefing) for teams or MTSs
★ Contingency Planning for teams and MTSs

★ Strategy 2: Use a counterfactual thinking approach to get team members, and teams in an MTS, to share their unique information

★ Strategy 3: Engage teams and MTSs in structured debriefing with feedback

Strategy 4: Develop adaptive thinking by providing exploratory or active learning experiences with wide problem variety

★ Strategy 5: Train leaders to pre-plan strategies for how multiple teams will work together

Strategy 6: Staff your CSIRT with team members who have a team orientation and teamwork skills.

CHAPTER 8: SHARED KNOWLEDGE OF UNIQUE EXPERTISE

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. My team members know exactly who has the knowledge to handle a particular incident.
2. My team members can explain "who knows what" within the team.
3. Members of my team ask the right person for information.
4. In team meetings, members appear to know what other people within the team know.
5. Members of my team communicate what knowledge they possess to other team members.
6. My team members know exactly which team in our CSIRT MTS has the right knowledge/expertise to handle a particular incident.
7. My teams explain "which teams know what" within the CSIRT MTS.
8. Members of my team ask the right team in a CSIRT MTS for information.
9. Members of my team communicate what knowledge they possess to other teams in the CSIRT MTS.

IMPROVEMENT STRATEGIES

★ Strategy 1: Knowledge Tools

★ Strategy 2: Presentation (type of cross-training)

★ Strategy 3: Job Shadowing (type of cross-training)

Strategy 4: Position Rotation (type of cross-training)

CHAPTER 9: TRUST IN INCIDENT RESPONSE TEAMS AND MULTITEAM SYSTEMS

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. My team members feel confident about the competence of other members.
2. My team members feel comfortable relying on each other when resolving tough incidents.
3. My team members feel comfortable admitting mistakes or seeking advice without worrying about being judged or evaluated.
4. My team members share learning opportunities with other members.
5. My team members talk freely with each other about difficulties they are having with incidents.
6. My team members bring up tough problems and issues with each other.
7. Members of my team manage differences of opinion without creating tension.
8. Members of my team resolve disagreements about incident mitigation.
9. Members of my team are comfortable having debates about different approaches to incident mitigation.
10. Tension and anger are well managed among members of my team.
11. My team feels confident about the competence of other teams in a CSIRT MTS.
12. My team members feel comfortable relying on other teams in the CSIRT MTS when resolving tough incidents.
13. My team members share learning opportunities with members of other teams in the CSIRT MTS.
14. Members of my team talk freely with members from other teams in the CSIRT MTS about problems they are having with incidents.
15. Team members bring up tough problems and issues with members of other teams in the CSIRT MTS.
16. My team manages differences of opinion with other teams in the CSIRT MTS without creating tension.
17. Tension and anger are managed well between teams in my CSIRT MTS.

IMPROVEMENT STRATEGIES

Strategy 1: Provide structured opportunities for CSIRT members to learn about the expertise, experiences, and functional backgrounds of other members

★ Strategy 2: Establish clear individual, team, and MTS goals, roles, and performance standards

Strategy 3: Establish norms for communication transparency in teams and MTSs

★ Strategy 4: Utilize managerial actions that create a psychologically safe climate in the team and MTS

★ Strategy 5: Create opportunities for building strong social connections among CSIRT members to support conflict management

Strategy 6: Increase external connections and social networking to facilitate inter-team and inter-organization trust

CHAPTER 10: SUSTAINED ATTENTION AND FOCUS OVER TIME DURING INCIDENT RESPONSE

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. My employees pick up on critical incidents toward the end of their shifts.
2. My employees sustain their attention over the course of their shifts.
3. My employees express satisfaction with the current scheduling of shifts and the length of shifts.
4. My employees claim that shift scheduling leads to improvement in sustaining attention during their shifts.
5. My employees appear to be alert at the end of their shifts.
6. My employees remain focused when dealing with incidents that require overtime work or an extra shift.
7. My employees take the correct amount of breaks during their shifts.
8. After-action reviews have revealed success attributable to sustained attention on the part of an analyst.

IMPROVEMENT STRATEGIES

Strategy 1: Hire job applicants who display a capacity for sustained attention.
- Working memory task
- Brief vigilance (i.e., sustained attention) tasks

★ Strategy 2: Encourage employees to incorporate rest breaks into their shifts.
- Restorative settings
- Socialization

★ Strategy 3: Shift Design – Create a shift plan that reduces sleep disturbances and maximizes attentiveness.
- Work Shift Characteristics
  - Shift length (8-hour shifts recommended)
  - Shift rotation speed (Rapid shift rotations preferred)
  - Shift rotation direction (Forward shift rotation preferred)

CONTINUOUS LEARNING IN INCIDENT RESPONSE

ASSESSMENT EXERCISE

1= STRONGLY DISAGREE, 2= DISAGREE, 3= NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE

1. Team members keep up-to-date with developments in cybersecurity.
2. The design of cybersecurity personnel's work roles allows them to develop new skills.
3. Team members engage others outside of the organization to gain new knowledge and skills.
4. Team members maintain contacts with other cybersecurity professionals in order to learn new knowledge and skills.
5. Team members have the opportunity to try out new ideas and processes.
6. Teams discuss how they should interact differently as a result of previous incidents (e.g., in after action reviews).
7. Thinking about "lessons learned" regarding team interactions or after-action reviews occur in a timely manner after events.
8. Multiple teams working together have the opportunity to try new ideas or processes.
9. Teams participate in activities where they can make errors and learn from their mistakes without these errors being detrimental to the CSIRT's performance (e.g., during training sessions).
10. Multiteam information databases (e.g., a Wiki, information board) are used in events.
11. Multiteam information databases (e.g., a Wiki, information board) are used in training.

IMPROVEMENT STRATEGIES

Strategy 1: Select individuals who are creative and curious

Strategy 2: Engage employees' creativity and curiosity as a leader

Strategy 3: Facilitate reflection in teams (team reflexivity or team reflections and adaptation)

★ Strategy 4: Provide feedback in debriefings (After Action Reviews)

Strategy 5: As a leader, promote psychological safety

★ Strategy 6: Improve work design (e.g., feedback, autonomy) to enhance learning

Strategy 7: Create databases to store knowledge

Strategy 8: Use mentoring programs

Strategy 9: Train employees to build networking skills

Strategy 10: Train CSIRT professionals on how to establish a professional, developmental network

★ Strategy 11: Use guided discovery learning

★ Strategy 12: Use error management training

* See the corresponding chapters in this handbook for full descriptions of improvement strategies for each topic and how to implement them

Appendix C

Hiring and Training CSIRT Employees: Validation Considerations

Contents

C.1 Introduction

This Handbook has provided a number of suggestions for selection and training tools for CSIRT managers to use in order to improve the social maturity and performance effectiveness of their teams. However, before they can be used, they need to be validated as either truly predictive of performance or capable of increasing targeted skills. This appendix provides some basic information about selection test and training validation. Additional information can be found at the following websites:

- http://www.onetcenter.org/dl_files/empTestAsse.pdf
- http://www.uniformguidelines.com
- www.uniformguidelines.com
- https://www.eeoc.gov/policy/docs/factemployment_procedures.html

Please note that guidelines on the validation and use of selection tests and training protocols may vary from country to country. Accordingly, managers should also confer with their human resource management departments for more guidance on local laws and regulations, as well as on the application of principles described here and in the aforementioned websites.

C.2 Hiring Validation Considerations

Selection tests are required to be both reliable and valid before they can be used to hire candidates for CSIRT positions.

C.2.1 TEST RELIABILITY

The reliability of a selection test refers to the extent to which participants who take the test on multiple occasions exhibit similar scores across the test administrations (i.e., test-retest reliability). Reliability also refers to the degree to which participants garner similar scores across multiple items on the same test that purports to measure the same knowledge, skills, abilities or other attributes (i.e., internal consistency). Reliability is indexed on a .00 to 1.00 scale. Reliability estimates greater than .70 are considered acceptable, while estimates greater than .90 are consider excellent. When tests are reliable, they produce dependable and consistent information about the test takers. If you are using an unreliable test to select members of your CSIRT, you will not be able to make well-informed hiring decisions.

C.2.2 RELIABILITY IN CSIRT APPLICANT TESTING

When selecting an employment test for applicants to your CSIRT, consider using an "off the shelf" product that has been designed by a consulting firm. Specific tests are referred to in various chapters in the Handbook. Some examples are personality tests, problem-solving tests, or sustained attention tasks. The manuals for predesigned employment tests will typically include a technical section describing the reliability studies the test designers have conducted. When using an off the shelf product, be sure to select one that has undergone a rigorous process for testing reliability to ensure you will receive dependable and consistent information from the test. If you choose to design your own test, engaging a consultant or consulting firm to conduct a reliability study will increase the test credibility and reduce the potential for a test-related lawsuit.

C.2.3 TEST VALIDITY

A test's validity refers to (a) the extent to which it assesses the construct it is intended to measure (i.e., construct validity), b) the extent to which the test captures all elements of a targeted construct or KSAO (i.e., content validity), and (c) the extent to which the test predicts the job outcomes you are targeting as a manager (i.e., criterion-related validity). A valid test is one that measures the job specific characteristics employees need to be effective in the job. Accordingly, if a test is highly valid, you can assume that high scores by applicants on the test mean that they are likely to exhibit higher job performance. Using valid tests will provide business efficiency benefits and will demonstrate that you are picking employees for your team based on their potential to perform well on the job. When selecting or designing an employment test for your CSIRT, you will need to ensure that the test is valid for CSIRT work. The websites listed above provide procedures for assessing a test's construct, content, and criterion-related validity.

If you select a test designed by external vendors, you should acquire from these vendors information both about the validity of your selected test as well as highly detailed descriptions of the validation studies completed by the testing company. If, as a CSIRT manager, you choose to use an off the shelf test, you need to ensure that the pre-existing validity studies were conducted on job types that are similar to cybersecurity incident response, or other cybersecurity functions in the job you are selecting for. Tests that have been validated on very different kinds of jobs may not necessarily be validated for positions and job functions in CSIRTs. Job similarity can be determined by using a job analysis to define the job tasks and responsibilities ad comparing the results of such an analysis with the tasks and responsibilities of jobs validated for use of a particular test. If your job analysis shows that the CSIRT function or position job you're hiring for is similar in terms of the tasks and KSAOs to the job that was used in the validity study of a particular off-the-shelf test, you can make the argument that the validity of the test will generalize to your CSIRT. Thus, when deciding whether an off-the-shelf test would be valid within the context of your CSIRT, consider:

- *Validity evidence*. Does the test use validation procedures that are consistent with accepted standards and best practices?
- *Job similarity*. Were the validity studies conducted on a job that is similar to the job you're using the test for on your CSIRT in terms of the KSAOs required?

- *Fairness evidence.* Does the test tend to yield disproportionate rates of hiring for some groups of job applicants (e.g., in terms of gender, race, and age) over others? If your test appears to exhibit "adverse impact" against some groups (e.g., women, older applicants), the validity of the test becomes even more important in defending your hiring choices against litigation.

For a full discussion of the issues around validity in a U.S.-based context, refer to www.uniformguidelines.com. If you are hiring for your CSIRT outside the U.S., you must consider the employment discrimination standards and guidelines for the country in which the CSIRT is located. In some cases, the laws of multiple countries may apply (e.g., when a U.S. company hires employees in Germany).

C.2.4 FURTHER READING

This brief appendix is meant to be an overview of the issues that can arise when using an employment test. The Uniform Guidelines, and the other websites referenced above, will provide a much more in-depth examination of these and other issues.

C.3 Training Validation Considerations

Carefully planned and business-focused employee training practices help companies build their business and gain a competitive advantage. *Training* refers to efforts that a company takes to help employees learn the KSAOs they need to perform their jobs. For example, a CSIRT may engage in an employee training program on communication designed to give CSIRT members the skills to know when and how to communicate about incident response. To maximize the connection between training and the creation of competitive advantage, training must be linked to a business strategy or need and evaluated based on the performance change it creates in employees.

C.3.1 INCREASING THE PERFORMANCE IMPACT OF TRAINING

Noe (2010, p. 7) described a seven-step instructional design process that can foster effective training outcomes. These steps include:

1. Conduct a training needs assessment
2. Ensure employee training readiness
3. Create a learning environment
4. Garner training support
5. Develop an evaluation plan
6. Select training methods
7. Monitor and evaluate training effectiveness

1. Conduct Training Needs Assessment

A training needs assessment identifies the gaps that may exist in the skills of employees, relative to the needs of the organization. A needs assessment typically includes an examination and measurement of the current KSAO levels of the employees, the needs of the organization overall, and an identification of the tasks that the employees' specific jobs require. Training can then be designed to develop the employee KSAOs that are important to the organization.

On a CSIRT, the training needs assessment may include steps such as identifying technical skills that the employees may need to develop, the skills that the entire CSIRT may lack, and the types of incidents that the organization is expecting to encounter. These three examinations should result in an identification of the KSAOs that the CSIRT requires and that are not currently present in the employees. From here, the CSIRT managers can develop learning objectives and an instructional plan to train employees on the gaps that they need to fill to increase CSIRT performance.

2. Ensure Employee Training Readiness

For a training program to be successful, the employees must be interested in and ready to gain the skills that they will learn through the training. If the training program requires some preexisting knowledge, the trainees must already have that knowledge, and they must also be motivated and in the right mindset to learn from the training.

On a CSIRT, for example, if a training program is designed to develop communication skills between CSIRT component teams, the trainees must be interested and willing to work on between-team communication. They must also already have a base level of communication skills in order to be able to benefit from the more advanced training and to apply what they learn in the training program to the job.

3. Create a Learning Environment

In addition to ensuring that an employee is ready to acquire the KSAOs from a training program, the training must take place in an environment that facilitates learning. Aspects of a learning environment include (Noe, 2010):

- creating clear learning objectives for the trainees,
- making the material meaningful and job relevant,
- creating opportunities for practice and feedback, and
- administering the program at a time that employees are able to engage with the material and information (e.g., not during the middle of a complicated incident resolution process).

A learning environment will help your trainees use feedback and feel comfortable practicing what they learned in the training.

4. Garner Training Support

Transferring what the trainees have learned to the work they are doing on a daily basis involves making sure that the trainees' coworkers and managers are aware and supportive of the training program that they have just completed. The trainees' themselves must also have the self-management skills to actively focus on using the new KSAO on the job, instead of reverting back to old, comfortable ways of completing the work.

5. Develop an Evaluation Plan

A comprehensive evaluation plan will enable CSIRT managers to determine if the training is achieving their desired outcomes. Managers must determine exactly what they hope to see as a training outcome, and then determine how to measure the outcome. For example, if a CSIRT manager puts employees through a between-team communication training program, the expected outcome may be improved levels of between-team communication. The manager can measure this outcome by determining if between-team communication has improved following the training, relative to the amount and quality of between-team communication that was occurring before the training--and if the extent of improvement during this time is greater for teams who have been trained than for teams who have not. Training evaluation must be planned before training is started.

6. Select Training Method

The training delivery method must be matched to the content and goals of the training. Reviewing the learning objectives will help determine how training should be administered. For example, a CSIRT going through a training program to improve between-team email communication should include practice sessions that allow trainees to draft, edit, and send appropriate email communications. Cost of delivery method is also likely to factor into the decision about how training should be administered. When there are large numbers of trainees based in many different locations, a virtual training program may be the only practical option from a cost standpoint. In this case, managers should ensure that the material is appropriate for an online delivery method.

7. Monitor and Evaluate Training

The final step in designing a training program is to monitor and evaluate the training. The training should be evaluated against the outcomes that were selected during the development of the evaluation plan. Training programs can be evaluated using a four-tiered system, described below. [1]

- *Reaction*. Measures how the trainees felt about the training. Ideally, trainees will feel as though training was a valuable and worthwhile experience. Measuring reactions gives you the opportunity to identify areas or topics missing from training and improve training for future trainees. Consider asking your trainees the following questions:
  - Did you feel the training was successful?
  - What were the biggest strengths of the training program?
  - What were the biggest weaknesses of the training program?
  - Did you like the training venue?
  - Did you like the trainer's presentation style?
  - What would you change about the training for future trainees?
- *Learning*. Measures how much your trainees have learned from the training program. Compare trainee learning against the gaps in KSAOs that you identified during the training needs assessment. Consider measuring your trainees' KSAOs using a survey or performance evaluation before and after the training session so you can assess learning.
- *Behavior*. Measures how the trainees apply the material that they learned in the training to the job itself. Behavior change can be challenging to measure, and behavior change should be measured weeks or months after training is completed. Consider asking your trainees some questions like the ones below.
  - Were you able to put any of the training to use on your job in the weeks/months since the training program was completed?
  - Were you able to teach your team members anything that you learned in the training program?
- *Results*. Measures the outcomes that you determined would be good for business and/or good for your CSIRT. These outcomes should have been determined during the development of the training needs assessment and should be measured over the long term. For your CSIRT, you may consider results such as:
  - Number of incidents successfully handled
  - Incident resolution quality
  - Information shared between CSIRT members or teams

When implementing the evaluation method, consider that it can be expensive to measure the outcomes of behavior and results. The four levels of evaluation are considered to build on one another, so in order for behavior change to occur and results to be seen, trainees should have a positive reaction to and have learned from the training.

These seven steps constitute best practices for training design and delivery. Following the steps will help a training program achieve success and increase the chances that the employees who go through the training will be able to transfer what they learned to the job. This brief appendix is designed to provide an overview of the steps required to design and deliver training; however it is not an in-depth examination of any of the steps. CSIRT managers should consider working with a consultant or consulting firm that has experience creating and administering training programs to CSIRTs.

C.3.2 FURTHER READING

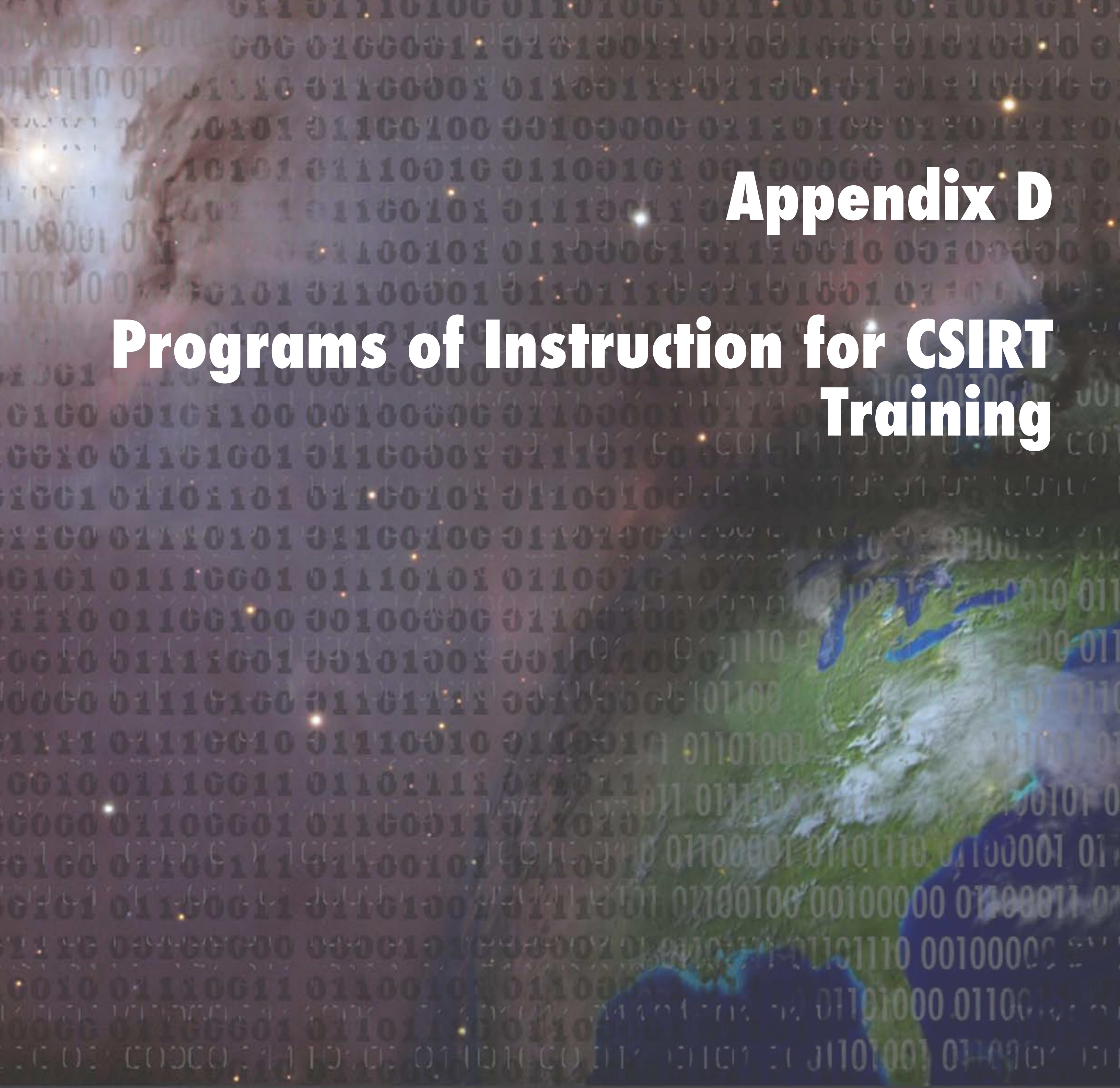
Further information and resources for training development can be found at the Association for Talent Development website www.td.org.

References

Kirkpatrick, D.L. (1994). Evaluating training programs: The four levels. San Francisco: Berrett-Koehler.

Noe, R.A. (2010). Employee training and development. New York, NY: McGraw Hill.

[1] Kirkpatrick Four Level Training Evaluation Model: Kirkpatrick, D. L. (1994). *Evaluating training programs: The four levels*. San Francisco: Berrett-Koehler.



Appendix D

Programs of Instruction for CSIRT Training

In this appendix, we have included four Programs of Instruction (POIs) to indicate how particular training programs suggested in the handbook can be designed by CSIRT trainers. These four POIs include training in:

- Communication skills (Chapter 5)
- Team pre-planning and pre-briefing (Chapter 7)
- Development of shared knowledge of unique expertise (SKUE) (Chapter 8)
- Discovery learning and error management training (Chapter 11)

Please refer to the respective chapters indicated for additional details on each form of training. Also, if you would like assistance on the development and delivery of these and related training programs, please e-mail one of the following individuals at George Mason University, Fairfax, Virginia, USA:

Dr. Stephen Zaccaro: szaccaro@gmu.edu
Dr. Lois Tetrick: ltetrick@gmu.edu
Dr. Reeshad Dalal: rdalal@gmu.edu

PROGRAM OF INSTRUCTION FOR CSIRT COMMUNICATION TRAINING TWO DAY WORKSHOP	
DESCRIPTIONS OF MODULES	
MODULES	**CONTENT**
Module A *Workshop and Project Description* 15 minutes	• Introductions, overview, and outline of workshop • Summarize goals of workshop
Module B *Communication in Cyber Security Incident Response; An Overview of Issues and Problems* 60 minutes	• Discuss role of communication and information sharing in effective cyber security • Exercise: o Describe 2-3 examples of effective communication in your team during incident response o Describe 2-3 examples of ineffective communication in your team during incident response o As a full group, discuss and identify the key elements that contributed to both effective and ineffective responses
Module C *Principles of Effective Communication* 360 minutes (Each of the 6 principles will require one hour total of coverage. This module can be spread over 2 days)	• Engage in lecture/discussion of 6 principles of effective communication in cybersecurity incident response: o Relevance, o Quality, o Timeliness, o Frequency, o Information Flow, o Confirmation and Response • For each principle, provide the following: o Definition o Examples of effective and ineffective display of principles • Exercise: For each principle, trainees should be provided with 3-5 practice incident response scenarios in which they are to produce a piece of communication reflecting that principle. Trainers should provide feedback on each practice communication. • After exercise debrief: Trainees should indicate key insights gained from their practice scenarios and discuss lessons learned.
Module D *Simulation Exercise* 180 minutes (for 2 simulations)	• Exercise: The trainer should develop 2-3 extended incident response simulations in which trainees organized in teams are required to respond and communicate with one another and other teams during the course of an unfolding incident. The simulation should be structured to require multiple applications of all 6 communication principles. • After each simulation, the trainer should facilitate an after action review to provide feedback on displayed communication.
Module E *Team Communication Charters* 150 minutes	• This module is intended to help managers to set up communication charters that facilitate effective team communication and information sharing. • Lecture/discussion of communication charters o Definition of communication team charters o Examples of effective CSIRT team charters • Exercise: Trainees simulate a new CSIRT and are tasked with developing a team communication charter. • After exercise debrief: Trainers should provide feedback on the developed team charters. Trainees should indicate key insights gained from their sessions.

PROGRAM OF INSTRUCTION FOR CSIRT COMMUNICATION TRAINING (CONTINUED)
TWO DAY WORKSHOP

DESCRIPTIONS OF MODULES

MODULES	CONTENT
Module F Taking it Home 60 minutes	• Work on training transfer to the workplace. • The goal of this module is to teach trainees to apply the communication principles and communication charters they discussed in the workshop to their jobs. • Exercise: o Choose principles of communication that they want to work on/facilitate back at the worksite o Develop a list of tools/tips/resources they will utilize. o Consider change obstacles and come up with strategies for addressing obstacles.
Module G Wrap-up 15 minutes	• Recap of key principles from the workshop and their application. • Description of additional team communication resources. • Feedback and evaluation of workshop.

PROGRAM OF INSTRUCTION FOR INCIDENT RESPONSE PRE-BRIEFING
SIX HOUR WORKSHOP

DESCRIPTIONS OF MODULES

MODULES	CONTENT
Module A *Workshop and Project Description* 30 minutes	• Introductions, overview, and outline of workshop • Describe pre-briefing to workshop participants • Provide evidence of pre-briefing effectiveness • Summarize goals of the workshop
Module B *In-depth description of pre-briefing* 90 minutes	• Define pre-briefing o Advantages of pre-briefing • Improved shared understanding • Higher team effectiveness o Pre-briefing forms for CSIRTs o Virtual whiteboards o Pre-briefing worksheets with prompts that encourage team members to share critical knowledge about an incident o Examples of CSIRT pre-briefing (both effective and ineffective) • Discussion of pre-briefing applicability to workshop participants o Participants provide their own experience with pre-briefing, describing virtual whiteboards, worksheets, and other tools they have used for pre-briefing.
Module C *Pre-briefing exercise* 150 minutes	• Work in groups to complete a pre-briefing exercise • Exercise: o Provide an example incident to trainees o Select an incident that your CSIRT recently solved; it's especially helpful if you can select an incident where information was not shared effectively between teams to highlight how pre-briefing would have helped in this situation o Ensure that all trainees understand the incident and are ready to engage in the exercise o Trainees complete pre-briefing prompt worksheet, attached to this workshop o Pre-briefing prompt worksheet can include phrases such as "you have the responsibility to tell your teammates what you know to help the incident get resolved. What information do you have about the incident that will help your teammates?" o Debrief exercise o Review and discuss prompt responses o Discuss lessons learned and job applicability
Module D *Taking it Home* 75 minutes	• Work on training transfer to the workplace • The goal of this module is to teach trainees to apply the pre-briefing strategies discussed in the workshop • Exercise: o Participants each choose a concept of pre-briefing that they want to work on/facilitate back at their worksite, using the worksheet attached o Develop a list of tools/tips/resources they will utilize o Consider change obstacles and come up with strategies for addressing obstacles

PROGRAM OF INSTRUCTION FOR INCIDENT RESPONSE PRE-BRIEFING (CONTINUED)	
SIX HOUR WORKSHOP	
DESCRIPTIONS OF MODULES	
MODULES	CONTENT
Module E *Wrap-up* 15 minutes	• Recap of pre-briefing application • Description of additional pre-briefing resources • Feedback and evaluation of workshop

MODULE C TEMPLATE	
PRE-BRIEFING EXERCISE	
THINK OF AN INCIDENT THAT YOUR TEAM RECENTLY HAD TO SOLVE AND FILL OUT THE WORKSHEET BELOW	
Incident Description	
What information was shared between teams?	
What information was not shared between teams that would have helped incident resolution?	
Create 2-3 pre-briefing prompts that would have helped with information exchange (e.g. What information do you have that will help your teammates)?	

MODULE D TEMPLATE PRE-BRIEFING APPLICATION
Choose a pre-briefing concept that you have learned today and describe how you can use it the next time you are working on a complicated incident.
What resources (e.g., people, programs, etc.) can you use to help you make your pre-briefing successful?
What obstacles might you encounter in your pre-briefing efforts and how would you overcome them?

PROGRAM OF INSTRUCTION FOR DEVELOPING SHARED KNOWLEDGE OF UNIQUE EXPERTISE (SKUE)	
THREE HOUR WORKSHOP	
NOTE: THIS TRAINING PROGRAM SHOULD BE COMPLETED WITH INTACT CSIRTS IN WHICH THE DEVELOPMENT OF SKUE HAS BEEN DEEMED A NECESSARY LEARNING OBJECTIVE	
MODULES	CONTENT
Module A *Workshop and Project Description* 30 minutes	• Introductions, overview, and outline of workshop • Describe shared knowledge of unique expertise (SKUE) to workshop participants • Provide evidence of SKUE advantages • Summarize goals of the workshop
Module B *In-depth description of SKUE* 60 minutes	• Define SKUE o Shared Knowledge of Unique Expertise o Unique expertise includes any experience or knowledge that a team member brings to the team o When other team members are aware of this knowledge or experience, they can leverage it for incident resolution • Advantages of SKUE for CSIRTs o For recently formed CSIRTs, or for CSIRTs who may have changing membership, building the perception of team member competence through an understanding of the expertise of each team member will help build trust o Increasing team member knowledge of the skills that other team members possess will enable team members to quickly call on the appropriate person when faced with an unfamiliar incident • Discuss SKUE applicability to workshop participants o Participants provide their own experience with having an (un)awareness of team member experience and how it has helped (or hindered) incident response in the past

PROGRAM OF INSTRUCTION FOR DEVELOPING SHARED KNOWLEDGE OF UNIQUE EXPERTISE (SKUE) (CONTINUED)

THREE HOUR WORKSHOP

NOTE: THIS TRAINING PROGRAM SHOULD BE COMPLETED WITH INTACT CSIRTS IN WHICH THE DEVELOPMENT OF SKUE HAS BEEN DEEMED A NECESSARY LEARNING OBJECTIVE

MODULES	CONTENT
Module C *Cross-Training on Team Member Expertise* 60 minutes	• Work in groups to complete a SKUE cross-training exercise • Exercise: o CSIRT trainees pair off and ask each other questions to gain an understanding of each other's career history, CSIRT-related experience, and special skills o Questions may include: • Where did you work before coming here? • What are three strengths you bring to the team? • What specialized knowledge do you have? • What education or training do you have? • Do you have any areas of particular interest that you have done self-development to learn about? o CSIRT trainees then describe the skills and unique expertise of their partner to the group while a designated note taker records each member's skills or experience in the worksheet below o Debrief exercise o Review and discuss lessons learned o How this new knowledge can be applied to the CSIRT?
Module D *Knowledge Bank Creation Planning and Wrap-Up* 30 minutes	• The last exercise gave trainees a greater understanding of the unique expertise each team member brings to the CSIRT o One of the trainees was a designated note taker o Now this information can be stored and maintained in an online knowledge bank o The goal of module D is to decide on a plan for retaining and maintaining this newly compiled knowledge o A trainee can be designated as the knowledge manager and ensure that the unique expertise of team members is stored in an easily accessible place • Provide feedback and evaluate the workshop

MODULE C NOTE TAKING TEMPLATE

SKUE NOTE TAKING FORM

TEAM MEMBER NAME	UNIQUE EXPERTISE

DISCOVERY LEARNING AND ERROR MANAGEMENT TRAINING [1]
PROGRAM OF INSTRUCTION

CSIRT members can develop the ability to adapt to new and changing situations by implementing specific guidelines that will help them prepare for unfamiliar situations and develop the skills to adapt, as individuals and as a team, to the variety of challenges they may encounter during incident resolution.

GUIDELINE	IMPLEMENTATION
Create open exercises to encourage self-directed learning.	• Trainees will benefit from exercises that require them to figure out creative solutions to problems. • As a manager, use exercises that facilitate learning in trainees by enabling them to work toward their own solution and not follow a set of pre-determined steps. • Open exercises will help trainees learn to think creatively about problems when they are back on the job.
Create challenging exercises to stretch trainee knowledge.	• Training exercises should push trainees to learn new knowledge or ways of solving problems. • As a manager, you should be mindful of the current level of skill in your trainee before determining the training assignment. Select assignments that are challenging but not beyond their abilities. • Once trainees solve a difficult exercise, they will build confidence and the skills to think about incident response in more complex ways.
Frame trainee mistakes as learning opportunities.	• Trainees gain confidence and knowledge when they are able to learn from their own mistakes. • As a manager, when employees make mistakes, frame them as learning opportunities. Discuss the situation, the lesson to be learned, and help your employee see mistakes in a positive light--as a chance to improve. • When trainees know that they have a manager's support, they will be more willing to admit to mistakes (rather than cover them up). Sharing past errors, as well as their resolution, can become a learning opportunity for the whole CSIRT.
Create exercises that require developing different solutions to foster adaptability.	• Trainees can develop adaptability by considering the way they would typically respond to a challenge or issue, and then thinking of a different response, called "frame-switching". • As a manager, to develop the frame-switching abilities of your team, create training exercises that require different solutions. • Developing frame-switching capabilities will help trainees avoid getting stuck in their typical set of responses when they encounter novel problems on the job.
Provide constructive feedback at appropriate moments during the training exercise.	• Specific, actionable feedback during training exercises encourages trainees to adjust their tactics during the training exercises. • As a manager, you can provide training feedback that guides your employees to change the ways that they are working on the exercise. • When feedback is specific and encourages new ways of problem-solving, trainees can apply the feedback to their jobs, teaching them to think creatively during incident response.
Plan for a reflection period after the exercise is completed.	• After a training exercise, trainees can use a reflection period to discuss successes and lessons learned. • As a manager, create a judgment-free environment to discuss the exercise and learn. • This reflection period provides an opportunity to ensure trainees can apply the lessons from training to the future incident resolution.

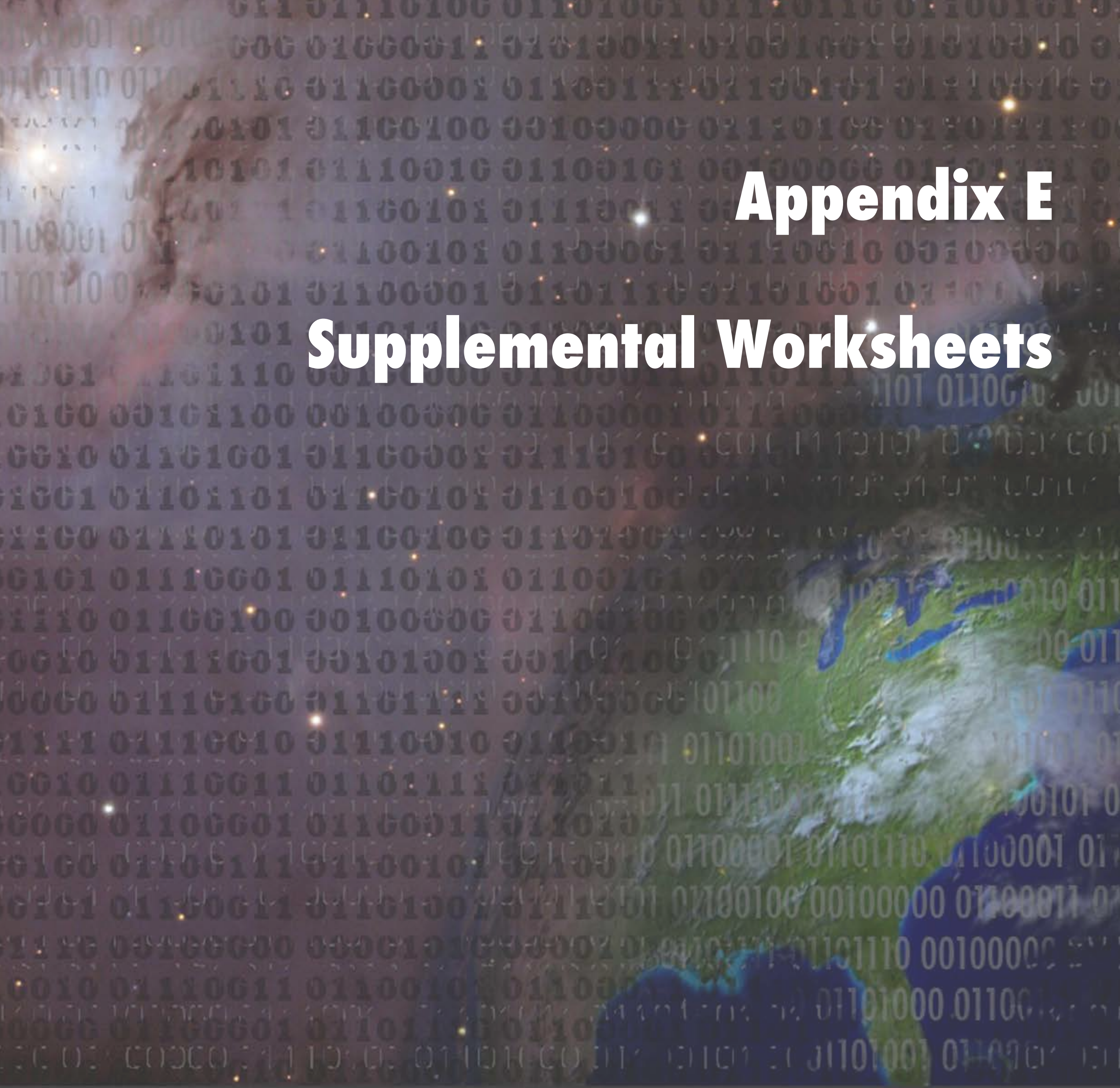
[1] Further reading:

Bell, B.S. & Kozlowski, S.W. (2002). Adaptive Guidance: Enhancing Self-Regulation, Knowledge, and Performance in Technology-Based Training. *Personnel Psychology, 55*: 267-306.

Kozlowski, S.W. J. & Bell, B. S. (2008). Team learning, development, and adaptation. In V. I. Sessa & M. London (Eds.), *Group learning (pp. 15-44)*. Mahwah, NJ. LEA.

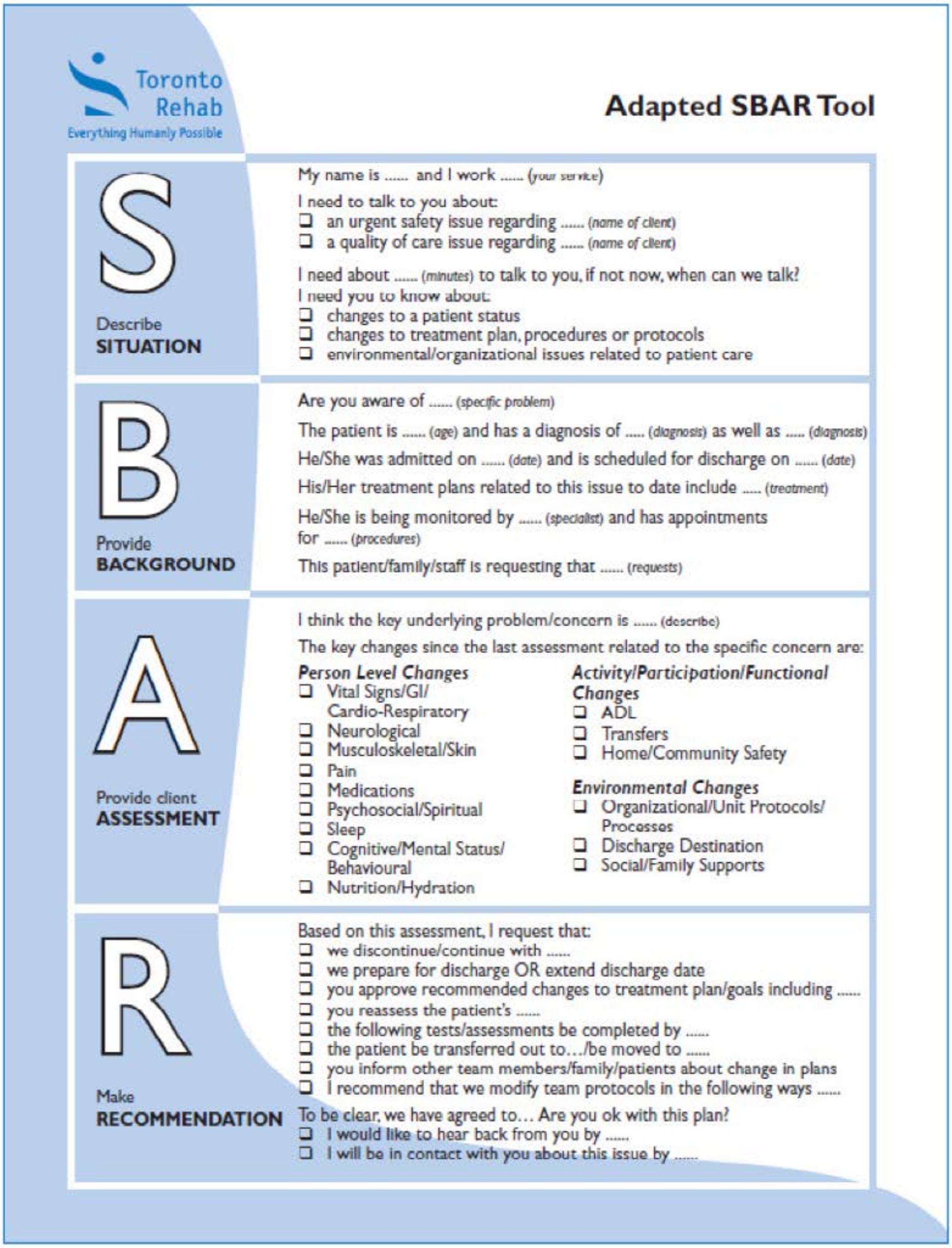
Keith, N. & Frese, M. (2008). Effectiveness of Error Management Training: A Meta-Analysis. *Journal of Applied Psychology, 93*, 59-69.

Steele-Johnson, D. & Kalinoski, Z. (2014). Error framing effects on performance: Cognitive, motivational, and affective pathways. *Journal of Psychology, 148*, 93-111.



Appendix E

Supplemental Worksheets



Toronto Rehab
Everything Humanly Possible

Adapted SBAR Tool

S

Describe
SITUATION

My name is ...... and I work ...... *(your service)*

I need to talk to you about:
- ❑ an urgent safety issue regarding ...... *(name of client)*
- ❑ a quality of care issue regarding ...... *(name of client)*

I need about ...... *(minutes)* to talk to you, if not now, when can we talk?
I need you to know about:
- ❑ changes to a patient status
- ❑ changes to treatment plan, procedures or protocols
- ❑ environmental/organizational issues related to patient care

B

Provide
BACKGROUND

Are you aware of ...... *(specific problem)*

The patient is ...... *(age)* and has a diagnosis of ..... *(diagnosis)* as well as ..... *(diagnosis)*

He/She was admitted on ...... *(date)* and is scheduled for discharge on ...... *(date)*

His/Her treatment plans related to this issue to date include ..... *(treatment)*

He/She is being monitored by ...... *(specialist)* and has appointments for ...... *(procedures)*

This patient/family/staff is requesting that ...... *(requests)*

A

Provide client
ASSESSMENT

I think the key underlying problem/concern is ...... *(describe)*

The key changes since the last assessment related to the specific concern are:

Person Level Changes
- ❑ Vital Signs/GI/ Cardio-Respiratory
- ❑ Neurological
- ❑ Musculoskeletal/Skin
- ❑ Pain
- ❑ Medications
- ❑ Psychosocial/Spiritual
- ❑ Sleep
- ❑ Cognitive/Mental Status/ Behavioural
- ❑ Nutrition/Hydration

Activity/Participation/Functional Changes
- ❑ ADL
- ❑ Transfers
- ❑ Home/Community Safety

Environmental Changes
- ❑ Organizational/Unit Protocols/ Processes
- ❑ Discharge Destination
- ❑ Social/Family Supports

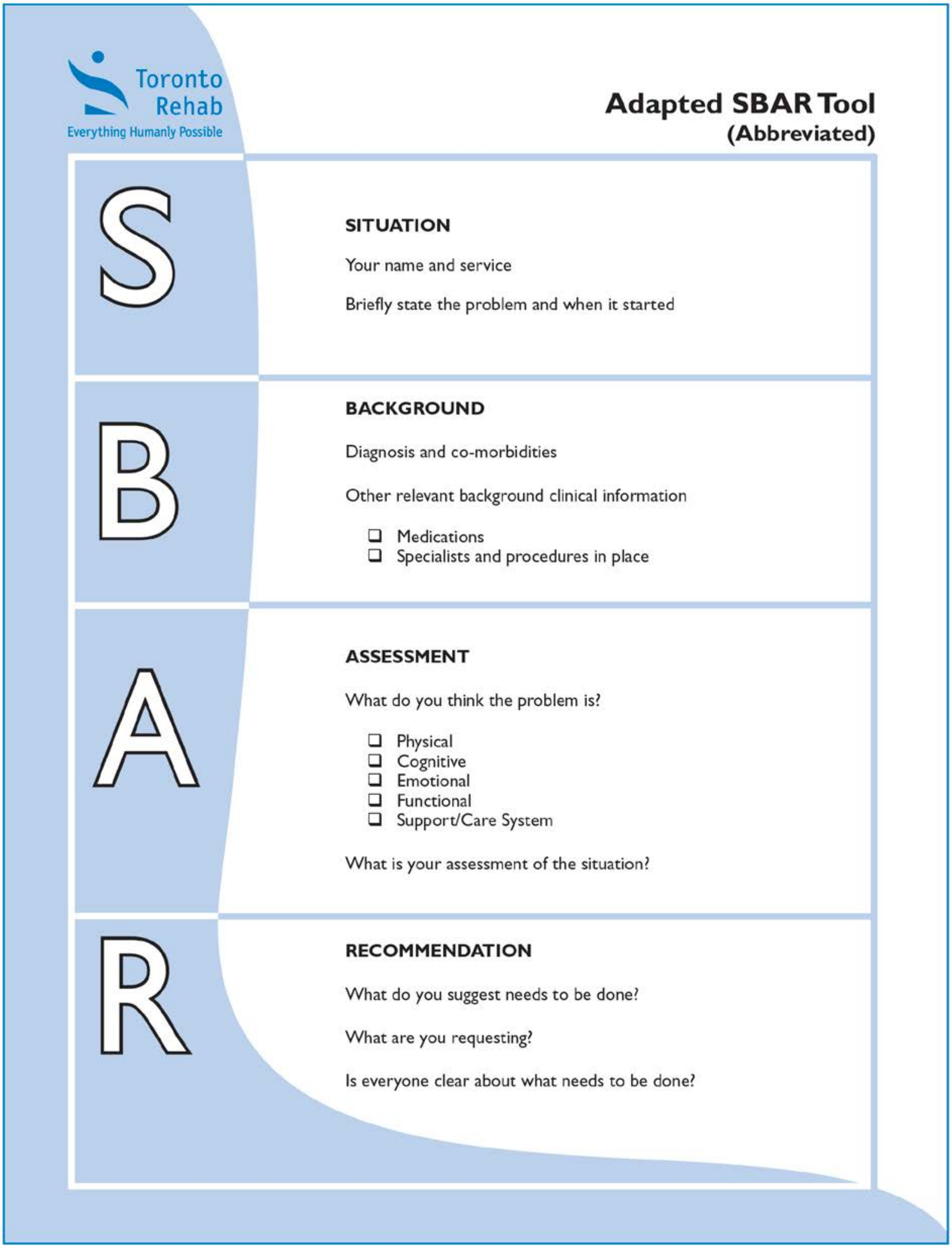
R

Make
RECOMMENDATION

Based on this assessment, I request that:
- ❑ we discontinue/continue with ......
- ❑ we prepare for discharge OR extend discharge date
- ❑ you approve recommended changes to treatment plan/goals including ......
- ❑ you reassess the patient's ......
- ❑ the following tests/assessments be completed by ......
- ❑ the patient be transferred out to…/be moved to ......
- ❑ you inform other team members/family/patients about change in plans
- ❑ I recommend that we modify team protocols in the following ways ......

To be clear, we have agreed to… Are you ok with this plan?
- ❑ I would like to hear back from you by ......
- ❑ I will be in contact with you about this issue by ......

Sample customized SBAR tool
Note: From "SBAR: A shared structure for effective team communication: 2nd Edition," by B. Trentham, A., Andreoli, N. Boaro, K. Velji and C. Fancott, 2010, p.4. Copyright 2010 by Toronto Rehabilitation Institute. Reprinted with permission.



Toronto Rehab
Everything Humanly Possible

Adapted SBAR Tool
(Abbreviated)

S

SITUATION

Your name and service

Briefly state the problem and when it started

B

BACKGROUND

Diagnosis and co-morbidities

Other relevant background clinical information

- ❑ Medications
- ❑ Specialists and procedures in place

A

ASSESSMENT

What do you think the problem is?

- ❑ Physical
- ❑ Cognitive
- ❑ Emotional
- ❑ Functional
- ❑ Support/Care System

What is your assessment of the situation?

R

RECOMMENDATION

What do you suggest needs to be done?

What are you requesting?

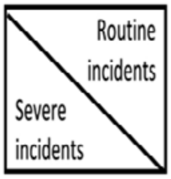
Is everyone clear about what needs to be done?

Sample abbreviated SBAR tool
Note: From "SBAR: A shared structure for effective team communication: 2nd Edition," by B. Trentham, A., Andreoli, N. Boaro, K. Velji and C. Fancott, 2010, p. 5. Copyright 2010 by Toronto Rehabilitation Institute. Reprinted with permission.

MTS Mapping Tool

Teams	1.	2.	3.	4.	5.	6.
1.	▨	▨	▨	▨	▨	▨
2.		▨	▨	▨	▨	▨
3.			▨	▨	▨	▨
4.				▨	▨	▨
5.					▨	▨
6.						▨
7 .						

Key: Interaction levels



1. ***Little or no interactions:*** Teams generally work separately
2. ***Moderate levels of interaction:*** One team passes work to the next team
3. ***High levels of interaction:*** Teams pass work back and forth until incident is resolved
4. ***Very high levels of interaction:*** Teams work closely together, often gathering and meeting in the same space.

Instructions

1. In the first column, list each team in your MTS. Please add more rows if your have more than 7 component teams in your MTS.
2. Repeat the list of teams in the top row, skipping team #7. If you have more than 7 teams in your MTS, please add an additional column for each team, skipping the last one.
3. In the upper right corner of each cell, using the key to indicate the typical or routine levels of interaction between the two teams
4. In the lower left corner of each cell, using the key to indicate the levels of interaction occurring between the two teams during high impact of severe cyber incidents.

EXAMPLE

Teams	1. Watch	2. Incident Res.	3. Malware	4. Forensics	5. Threat Intel.	6. Engineering
1. Watch						
2. Incident Response	2 3					
3. Malware Analysis	1 2	2 3				
4. Forensics	1 2	3 4	3 4			
5. Threat Intelligence	3 4	3 4	2 3	2 3		
6. Engineering	4 4	1 2	1 2	1 1	2 2	
7 Communications	1 1	2 3	2 3	2 3	2 3	2 2

Routine incidents

Severe incidents

Key: Interaction levels

1. ***Little or no interactions:*** Teams generally work separately.
2. ***Moderate levels of interaction:*** One team passes work to the next team.
3. ***High levels of interaction:*** Teams pass work back and forth until incident is resolved.
4. ***Very high levels of interaction:*** Teams work closely together, often gathering and meeting in the same space.

COLLABORATION TRIGGERING (E.G., SOCIAL MATURITY ASSESSMENT TOOL)	
ASSESSMENT EXERCISE	**SCORES**
1=STRONGLY DISAGREE, 2= DISAGREE, 3=NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE	
1. My analysts decide correctly that they should include other analysts in their incident mitigation efforts.	
2. Members of my team proactively solicit help from other team members.	
Average	
MULTITEAM SYSTEM COLLABORATION TRIGGERING	
3. My team solicits help from other teams in the CSIRT MTS.	
4. My team asks other teams in the CSIRT MTS to help them resolve an incident when such help is necessary.	
5. My team decides correctly that they should include other teams in the CSIRT MTS in their incident mitigation efforts.	
Average	

COMMUNICATION	
ASSESSMENT EXERCISE	**SCORES**
1=STRONGLY DISAGREE, 2= DISAGREE, 3=NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE	
1. Messages sent among my team members contain all critical information.	
2. Messages sent or received by the team are understood clearly.	
3. My team members ask for clarification for messages received from others when they are unsure of something.	
4. My team members confirm receipt and understanding of critical communications.	
5. Information is received on time when trying to address a cyber threat.	
6. Messages are sent to the correct recipient during different phases of incident resolution.	
7. Information is complete and accurate during handoffs between different individuals in my team.	
8. My team members quickly resolve communication issues with individuals in their teams.	
9. My team members quickly resolve communication issues with team members from other cultures.	
Average	
MULTITEAM SYSTEM COMMUNICATION	
10. Messages sent between my team and other teams contain all critical information.	
11. My teams ask for clarification for messages received from other teams when they are unsure of something.	
12. Confirmation of receipt and understanding of critical communications occurs between teams.	
13. Information is complete or accurate during handoffs between different teams.	
14. My teams quickly resolve communication issues with other teams.	
15. My teams designate a point person to communicate with other teams or external parties.	
Average	

COLLABORATIVE PROBLEM SOLVNING	
ASSESSMENT EXERCISE	SCORES
I=STRONGLY DISAGREE, 2= DISAGREE, 3=NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE	
I. Team members in my CSIRT proactively solicit help from each other.	
2. My team members get together to brainstorm and to consult each other about incident resolution.	
3. My team members use the knowledge they have gained from other team members in resolving a novel incident.	
4. My team members work together to determine the potential consequences of an event or threat to the cybersecurity of the organization or to constituents.	
Average	
MULTITEAM SYSTEM COLLABORATIVE PROBLEM SOLVING	
5. My team members incorporate the expertise of other teams into incident resolution.	
6. Teams in the CSIRT proactively solicit help from other teams.	
7. Multiple teams get together to brainstorm and to consult each other about incident resolution.	
8. Multiple teams work together to determine the potential consequences of an event or threat to the cybersecurity of the organization or to constituents.	
Average	

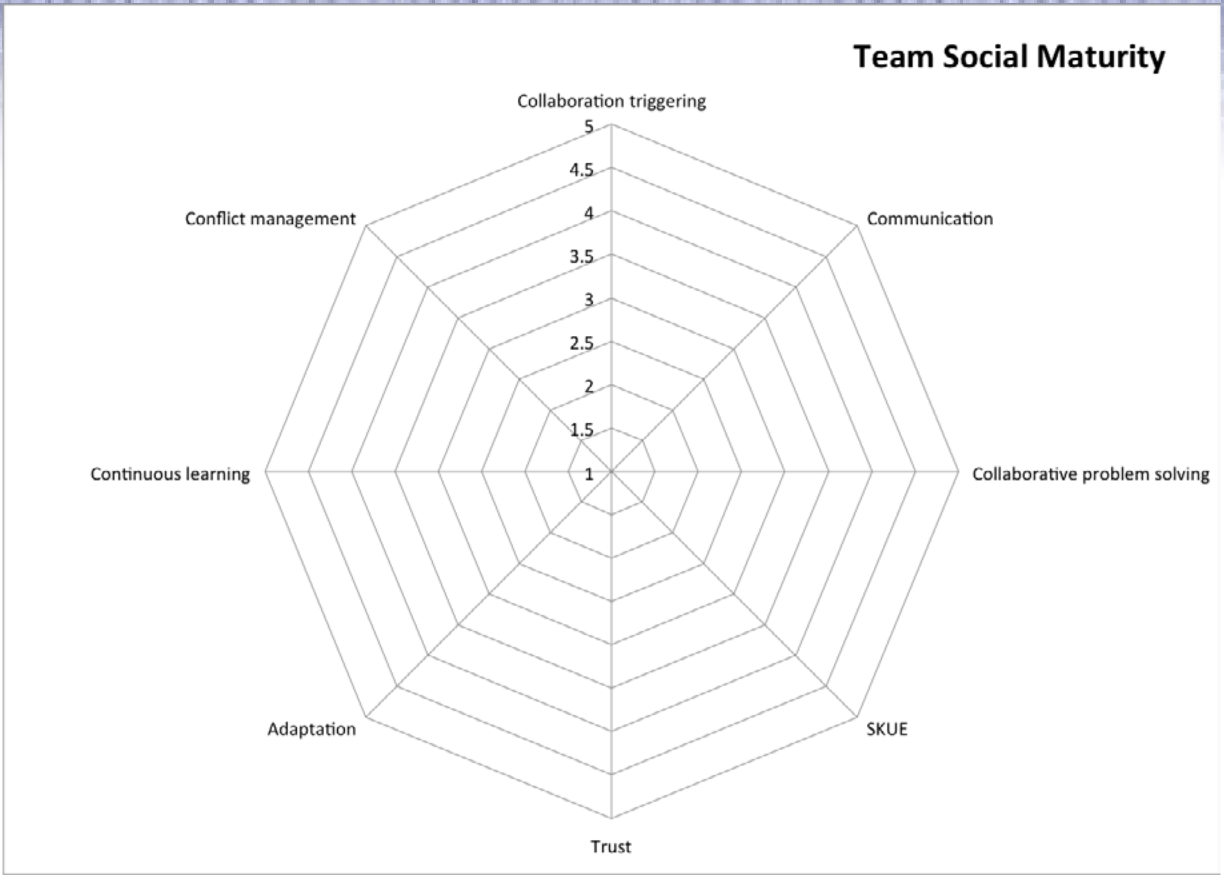
SHARED KNOWLEDGE OF UNIQUE EXPERTISE (SKUE)	
ASSESSMENT EXERCISE	SCORES
I=STRONGLY DISAGREE, 2= DISAGREE, 3=NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE	
I. My team members know exactly who has the knowledge to handle a particular incident.	
2. My team members can explain "who knows what" within the team.	
3. Members of the team ask the right person for information.	
4. In team meetings, members appear to know what other people within the team know.	
5. Members of my team communicate what knowledge they possess to other team members.	
Average	
MULTITEAM SYSTEM SKUE	
6. My team members know exactly which teams have the right knowledge to handle a particular incident.	
7. My teams can explain "which teams know what" within the CSIRT MTS.	
8. Members of the team ask the right team in a CSIRT MTS for information.	
9. Members of the team communicate what knowledge they possess to other teams in the CSIRT MTS.	
Average	

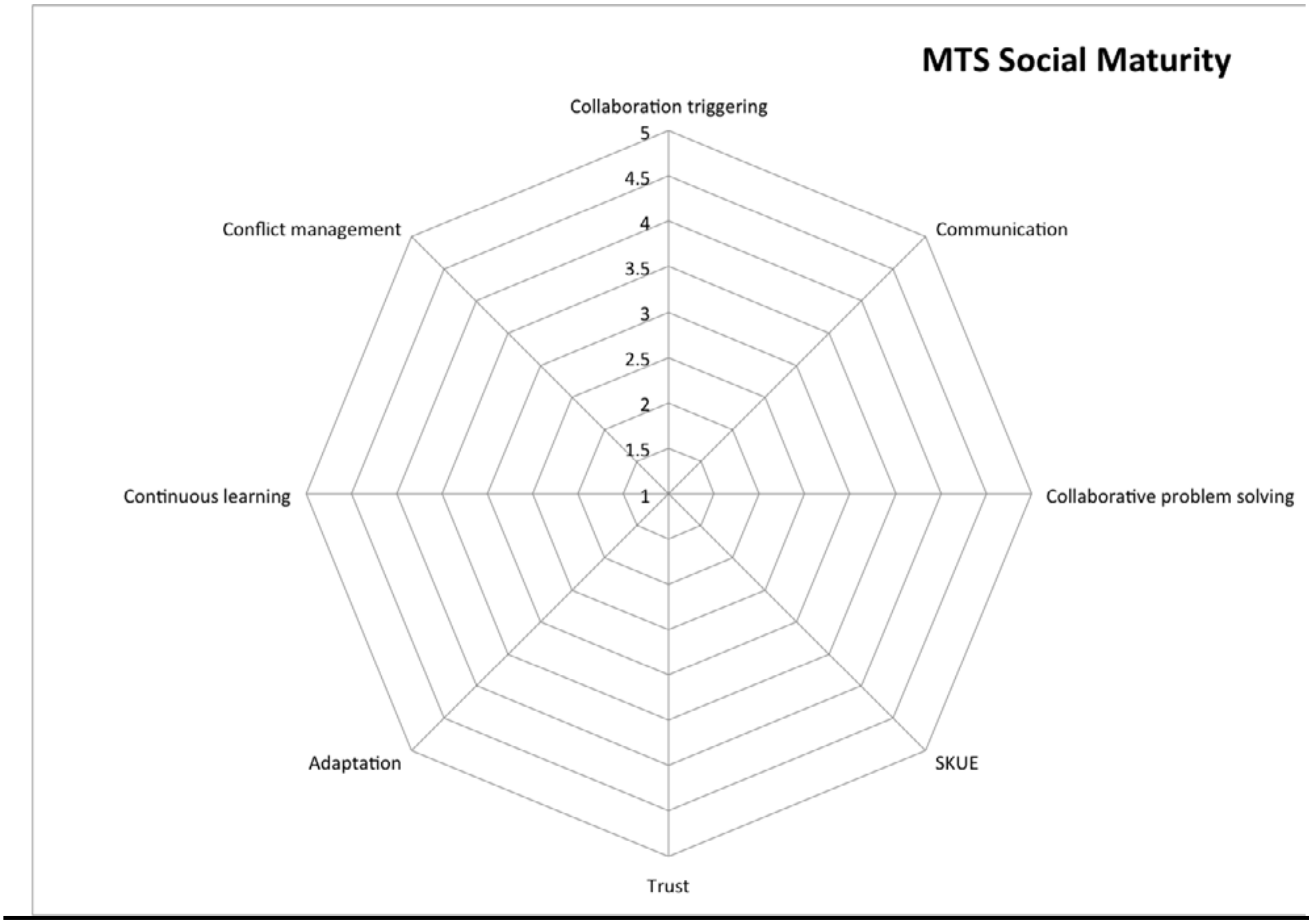
TRUST	
ASSESSMENT EXERCISE	SCORES
1=STRONGLY DISAGREE, 2= DISAGREE, 3=NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE	
1. My team members feel confident about the competence of other members.	
2. My team members feel comfortable relying on each other when resolving tough incidents.	
3. My team members feel comfortable admitting mistakes or seeking advice without worrying about being judged or evaluated.	
4. My team members share learning opportunities with other members.	
5. My team members talk freely with each other about difficulties they are having with incidents.	
6. My team members bring up tough problems and issues with each other.	
Average	
MULTITEAM SYSTEM TRUST	
7. My team feels confident about the competence of other teams in the CSIRT MTS.	
8. My team members feel comfortable relying on other teams in the CSIRT MTS when resolving tough incidents.	
9. My team members share learning opportunities with members of other teams in the CSIRT MTS.	
10. My team members talk freely with members from other teams in the MTS about difficulties they are having with incidents.	
11. My team members bring up tough problems and issues with members of other teams in the MTS.	
Average	

ADAPTATION	
ASSESSMENT EXERCISE	SCORES
1=STRONGLY DISAGREE, 2= DISAGREE, 3=NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE	
1. Members of my CSIRT consider multiple viewpoints when resolving an incident.	
2. Members of my CSIRT are willing to switch to new kinds of solutions when existing ones may not be the best.	
3. Members of my CSIRT try new ways of thinking about novel events and incidents.	
4. Members of my CSIRT adopt new ways of resolving incidents.	
5. Members of my CSIRT are comfortable with deviating from normal or typical ways of resolving incidents.	
6. My team members change their behaviors or protocols as a result of previous incidents.	
7. Members of my team are likely to try new ideas and solutions when resolving incidents.	
Average	
MULTITEAM SYSTEM ADAPTATION	
8. Teams in the CSIRT MTS change their ways of interacting with one another as a result of previous incidents.	

CONTINUOUS LEARNING	
ASSESSMENT EXERCISE	SCORES
1=STRONGLY DISAGREE, 2= DISAGREE, 3=NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE	
1. Team members keep up-to-date with developments in cybersecurity.	
2. The design of cybersecurity personnel's work roles allows them to develop new skills.	
3. Team members engage others outside of the organization to gain new knowledge and skills.	
4. Team members maintain contacts with other cybersecurity professionals in order to learn new knowledge and skills.	
5. Team members have the opportunity to try out new ideas and processes.	
Average	
MULTITEAM SYSTEM LEARNING	
6. Teams discuss how they should interact differently as a result of previous incidents (e.g., in after action reviews).	
7. Thinking about "lessons learned" regarding team interactions or after-action reviews occur in a timely manner after events.	
8. Multiple teams working together have the opportunity to try new ideas or processes.	
9. Teams participate in activities where they can make errors and learn from their mistakes without these errors being detrimental to the CSIRT's performance (e.g., during training sessions).	
10. Multiteam information databases (e.g., a Wiki, information board) are used in events.	
11. Multiteam information databases (e.g., a Wiki, information board) are used in training.	
Average	

CONFLICT MANAGEMENT	
ASSESSMENT EXERCISE	SCORES
1=STRONGLY DISAGREE, 2= DISAGREE, 3=NEITHER AGREE NOR DISAGREE, 4= AGREE, 5= STRONGLY AGREE	
1. Members of my team manage differences of opinion without creating tension.	
2. Members of my team resolve disagreements about incident mitigation.	
3. Members of my team are comfortable having debates about different approaches to incident mitigation.	
4. Tension and anger among my team members are well managed.	
Average	
MULTITEAM SYSTEM CONFLICT MANAGEMENT	
5. My team manages differences of opinion with other teams in the CSIRT MTS without creating tension.	
6. My team resolves disagreements with other teams in the CSIRT MTS about incident mitigation.	
7. Tension and anger are well-managed between teams in the CSIRT MTS.	
Average	


Team Social Maturity
Collaboration triggering
5
4.5
4
3.5
3
2.5
2
1.5
1
Communication
Collaborative problem solving
SKUE
Trust
Adaptation
Continuous learning
Conflict management


MTS Social Maturity
Collaboration triggering
5
4.5
4
3.5
3
2.5
2
1.5
1
Communication
Collaborative problem solving
SKUE
Trust
Adaptation
Continuous learning
Conflict management

Appendix F

Leveraging Strategies from Three Emergency Response Teams to Improve Cybersecurity Incident Response Team Effectiveness

Contents

F.1 Executive Summary

The effective functioning of cybersecurity incident response teams (CSIRTs) is critical to ensuring the security of organizations' infomational assets in today's interconnected computing environments. CSIRT history dates back to the 1988 Robert Morris worm, the world's first widespread cybersecurity incident (Whitman, Mattord, & Green 2007). Although CSIRT work has been in existence for several decades, the majority of research has focused on technology or the individual skills of analysts in the team, not teamwork itself.

Fortunately, other industries have already adopted strategies to help improve the effectiveness of their teams, which can be used to create a framework of best practices for CSIRTs. CSIRTs can learn from other emergency responders with different functions, but similar characteristics to CSIRTs, and can improve their effectiveness by adapting those teams' best practices. The focus of the current appendix is to examine three such teams: military response (MR), emergency medical service (EMS), and nuclear power plant operator (NPPO) teams.

From the research on MR teams, we recommend strategies CSIRTs can use to improve their ability to adapt (critical thinking training, stress exposure training, and perturbation training), to develop shared mental models (guided team self-correction and the commander's intent method), to communicate (briefing), and to employ trust-building behaviors. From EMS teams, we present ways CSIRTs can learn to improve their communication (checklists, handoff protocols, and wrap-up forms) and ways CSIRTs can encourage trust (development of team norms). Finally, from NPPO teams, we show how CSIRTs can learn to improve shared mental models cross-training and after-action reviews. To help managers and leaders understand what recommendations are best for their teams, we provide guidance on which recommendations should be favored for various situations based on each strategy's relative cost and effectiveness.

F.2 Introduction

Cyber networks across the globe are under near constant attack. According to a survey conducted by the Computer Security Institute (CSI), 90% of the participating organizations and government agencies detected network breaches within the preceding 12 months, and 80% of those detected breaches resulted in significant (acknowledged) financial loss (Peake, 2003). For example, the 2013 Target Corp. cyber attack, which granted attackers access to the credit card information of 40 million customers, and the 2015 Anthem cyber attack, which disclosed social security numbers and other sensitive information of 80 million individuals, cost both of those organizations significant sums in immediate damages, loss of reputation, and potential future sales.

These kinds of massive data breaches highlight why effective cybersecurity responses are so necessary to protect a group's (e.g., organization's, school's, nation state's) data and network. While many aspects of cybersecurity responses are focused on individual actions and skills—like how to identify possible incidents and when to investigate an event further—at its core, cybersecurity incident response requires teamwork, which is defined as a coordinated effort among many individuals whose shared goal is to protect a network from attacks (Chen et al., 2014). For example, when responding to an incident, team members might first collaborate to determine the nature of an incident, and then pass it along to others who assess the severity of the incident and decide how it should be resolved. Furthermore, when a severe incident is discovered, several teams may work together, simultaneously providing feedback to one another in order to understand the root cause of the incident while communicating critical information to others within and outside the team. Thus, the effectiveness of CSIRTs relies not only on their technological resources (e.g., system infrastructure) and individual analyst skills, but also on the team members' ability to function well with others. However, because of CSIRTs' relatively recent formation, the current body of knowledge about how to optimize team-related CSIRT functions is rather limited compared to what we know about other teams with similar core operating characteristics.

We do know that action teams like CSIRTs must be adaptive, must communicate, must trust each other, and must have a shared understanding of work tasks in order to be effective. Three teams that share these common characteristics (MR, EMS, NPPO) have been around much longer, and have been studied extensively in the behavioral sciences. Research into each of these teams has produced strategies for improving teamwork abilities and results, which CSIRTs can utilize to bring about positive change in their own teams.

In this paper, we first describe CSIRTs in more detail. Then, we introduce each of the three analogous teams alongside the strategies that can be adopted by CSIRTs, and we offer advice on when a CSIRT should favor one strategy over others. Throughout, we provide cost and effectiveness information on each recommended strategy. Measures of effectiveness (i.e., percent change in a given performance metric) were taken from various published peer-reviewed and technical documents that looked at improving team effectiveness in MR, EMS, or NPPO teams. Following previous research standards for similar cost-effectiveness analyses (e.g., Ryan & Tippins, 2004), estimates of cost were broken down into development and implementation categories. Final cost estimates were derived from a combination of direct references in scholarly works, technical manuals, published works on similar teamwork strategies, and expert knowledge of organizational effectiveness tools.

A paper related to the topic of this appendix was recently published in IEEE Privacy & Security (Steinke, et al., 2015). The present appendix, however, provides a considerable amount of additional information: for instance, a larger number of recommended strategies, a more in-depth description of each of the recommended strategies, more detail about how the recommended strategies can be put into practice in CSIRTs (including ways for managers to overcome resistance to change), more emphasis on comparing the costs and benefits of the recommended strategies, and a discussion of how the needs of individual CSIRTs will determine the choice of strategies to implement.

F.2.1 CYBERSECURITY INCIDENT RESPONSE TEAMS (CSIRTs)

“CSIRTs are teams composed of two or more individuals who interact with each other as well as with information technology (IT) infrastructure, other IT personnel, end-users, management, and other CSIRTs to prepare for and respond to computer security incidents” (Steinke et al., 2015, p. 4). The incident response process involves four main steps: 1) preparation, 2) detection (identification) and analysis, 3) containment, eradication, and recovery, and 4) lessons learned and other post-incident activity (adapted from Kliarsky, 2011, p. 4; see also Scarfone, Grance, & Masone, 2008). Stated differently, CSIRTs are responsible for maintaining secure information systems for their constituencies (e.g., organization, client, nation state) as well as developing incident response plans to prevent and respond to various types of cyber attacks. While relatively routine incident response (e.g., blocking an IP address) both composes the majority of the events seen by a CSIRT and is generally handled by a single analyst, serious attacks (e.g., focused operations, advanced persistent threats) require a collaborative and coordinated response from many individuals across the CSIRT.

CSIRTs operate in complex environments, which organizational researchers define by high degree of information load, information diversity, uncertainty surrounding the nature of incidents, and time constraint (Campbell, 1988; Gladstein & Reilly, 1985; Schroder, Driver, & Streufert, 1967). In addition, CSIRTs’ operating environment is highly dynamic in the sense that the incident response processes can change rapidly as events unfold. CSIRT members typically start their actions at the individual analyst level and make decisions on how and when to collaborate with others based on their assessment of the situation (Chen et al., 2014). When collaboration is necessary, CSIRTs must develop seamless communication channels and plan their team actions in response to salient cues or events that may otherwise be severely detrimental to their current team performance.

Given the criticality of their role—protecting organizations’ online assets—it is important for CSIRTs to employ strategies that can improve their team effectiveness. However, the amount of research focusing on CSIRT effectiveness is relatively limited, and, therefore, CSIRTs can learn from research on MR, EMS, and NPPO team effectiveness.

F.3 Recommendations to Improve CSIRT Effectiveness

F.3.1 MILITARY RESPONSE TEAMS

Military Response (MR) teams are trained groups of military personnel that are deployable by the United States Armed Forces in response to life-threatening events (e.g., medical outbreak, natural disaster, terrorist attacks, mass casualty events) that take place not only in the United States but also (almost) anywhere in the world. MR teams, which can take a variety of names depending on their function (e.g., Joint Nuclear Accident and Incident Response Teams; Fleet Antiterrorism Security Teams; Marine Expeditionary Units; Navy SEAL Teams), must act quickly in rapidly developing situations, regardless of where they are and what changes occur (Cecchine, Morgan, Wermuth, Jackson, & Schaefer, 2013).

Like CSIRTs, MR teams are often faced with serious situations that develop at a quick pace where the team must develop an effective response strategy. They must also manage large volumes of information that they receive during mission preparation, execution, and upon completion (Dalenberg, Vogelaar, & Beersma, 2009; Sundstrom, DeMeuse, & Futrell, 1990). In addition, it is critical for MR teams to be able to clearly communicate mission-related information and coordinate specific tasks among their members (e.g., Lloyd, 2001). Thus, the strategies that have been developed to improve the effectiveness of MR teams can be leveraged by CSIRTs.

Adaptation strategies from MR teams. As cybersecurity organizations continually develop their incident detection systems and the technical knowledge of their analysts, their adversaries also continually learn and improve upon their capabilities. As a result, new incidents are likely to use an unknown method to harm or infiltrate a network. Yet, in such uncertain situations, CSIRTs are not entitled to longer incident response periods as the uncertainty increases. On the contrary, they must change their core performance strategy and take action within a short amount of time in order to protect their constituencies’ networks. In other words, CSIRTs must adapt to unexpected, and often novel, situations under high time constraints.

Adaptation is often defined as how a team changes its behavior in response to certain situational cues in order to achieve a previously defined goal (Burke, Stagl, Salas, Pierce, & Kendall, 2006). Adaptive performance requires teams to scan environmental dynamics, interpret changing conditions, and develop fundamentally different adjustment strategies to maintain effective performance (Burke, et al., 2006; Cannon-Bowers, Tannenbaum, Salas, & Volpe, 1995). According to the Army Capstone Concept (2009), one of the fundamental characteristics of all areas of the military—including MR teams—is operational adaptability. A person with operational adaptability “[has] flexibility of thought,… [is] comfortable with collaborative planning and decentralized execution, [has] a tolerance for ambiguity, and [has] the ability and willingness to make rapid adjustments according to the situation” (The Army Capstone Concept, 2009, p. i). As such, MR teams are adaptive in a variety of dangerous contexts (e.g., nuclear threats, natural disasters, enemy combat) in order to successfully complete their mission (Ramthun & Matkin, 2014).

Research on adaptive performance in the military has identified several important areas of focus. One such area of focus is the need to develop decision-making skills (Tucker & Gunther, 2009). Critical thinking training has specifically been shown to be effective in improving decision-making skills in unfamiliar situations in the military (Cohen, Freeman, & Thompson, 1998). **Critical thinking training** involves four components (Cohen et al., 1998): 1) an overview of critical thinking processes as well as creating, testing, and evaluating a story (a simplified version of a real world phenomenon) to improve situational understanding; 2) a focus on particular kinds of stories such as "hostile intent stories," which provide explanations for particular attacks (Cohen, Freeman, et al., 1998, p. 164); 3) a recommendation of a devil's advocate strategy--thinking about potential downsides or negative consequences for each action being considered while evaluating a story's plausibility and finding alternative reasons behind observations; 4) guidelines for deciding when to think critically (e.g., more in-depth), and when to act immediately, based on the situational factors such as the time available and consequences of taking action. This training protocol has the following instructional objectives: development of skills in situational assessment, story- or sense-making, determination of uncertainties, justification of assumptions, and contingency planning (van den Bosch, Helsdingen, & de Beer, 2004).

For CSIRTs, critical thinking training could improve adaptive performance regarding how to use the time available to make the most effective decisions in unfamiliar situations (Cohen, Freeman, et al., 1998). Specifically, this training would involve an experienced cybersecurity analyst providing guidelines (e.g., "you should have opened the ticket earlier") and asking questions (e.g., "how can you verify your decision that this is a severe incident?") to train the CSIRT members on four skills: 1) assessing the training scenarios in context (e.g., building a story by considering the events leading to the current situation) rather than in isolation; 2) identifying incomplete and conflicting information in the story that they built, which requires further data/evidence collection; 3) critiquing the story they constructed in order to uncover any hidden assumptions in the story for further evaluation; 4) deciding whether critical thinking is an appropriate next step or if immediate action is preferred (see van den Bosch et al., 2004 for more detailed instructions).

Critical thinking is most suitable in non-routine situations that have lower risks from decision-making delays (van den Bosch, et al., 2004). In such situations, Cohen, Freeman et al. (1998, p. 180) found that critical thinking training increased a number of performance metrics in the analyses of "attack scenarios," including the "number of factors considered in assessment" of the intent behind an attack (30% increase), the "number of conflicting pieces of evidence identified" (58%), the "number of explanations of conflict generated" (27%), and "the number of alternative assessments generated" (41%).

Critical thinking training requires moderately high levels of resources to both develop and implement. The majority of costs can be attributed to the time required to create appropriate scenarios, on the one hand, and the loss of productivity for those attending the training, on the other hand (Morrison, Moses, Fletcher, Roberts, & Quinkert, 2007). Also, a necessary step is to bring in subject matter experts, thus increasing the development cost, prior to designing the training to analyze the CSIRT members' problem solving, judgment and decision-making tasks (a process known as cognitive task analysis). Two other factors contributing to the implementation costs are: 1) the need for a skilled and qualified facilitator (either an internal leader or external specialist) to run the training session so that all possible assumptions or holes in how trainees interpret the various situations can be caught and properly addressed, and 2) the need for domain experts to evaluate the training outcomes (e.g., information processing) based on each specific scenario (van den Bosch et al., 2004). As a key learning opportunity for team members, taking the extra time to discuss these assumptions, and how to think more critically about a given situation, is vital to ensuring the effectiveness of the training as a whole. For more information on implementing critical thinking training, including the taxonomy of story types and further recommendations for when critical thinking is applicable, one can refer to Cohen, Freeman, et al. (1998) and van den Bosch et al. (2004).

Although learning how to think and adapt as a team is important, certain situations create high levels of stress, which inhibits the ability of members to work together as a team (Driskell, Salas, & Johnston, 1999). An effective strategy that CSIRTs can leverage from MR teams to manage stress is called stress exposure training.

The instructional objectives of **stress exposure training** include familiarizing the team with dynamic and high-stress environments as well as teaching team members the skills to maintain effective team functioning and task performance in such environments (Driskell, Salas, & Johnston, 1998). The protocol for such training involves exposing teams to repeated trials on the same incident in the same environment while decreasing the time they have to act (Driskell, et al., 1998). This training improved team performance by almost 20% in the military, and the benefits of stress exposure training were maintained in subsequent, novel stress and novel task conditions (Driskell et al., 1998; Driskell, Johnston, & Salas, 2001).

CSIRTs can create their own stress exposure training programs by having team members collectively identify and discuss particular past events for which they recall how stress significantly affected the outcome and then create exercises to help develop skills that would enable the team members to reduce those stressful reactions. For example, CSIRT members can suffer from stress when there are only a few analysts on staff and there is a sudden notification about a high profile incident but only a vague definition of the issue and an incomplete data set from which to work. Once the incident escalates, the management becomes involved and puts constant external stress on the team to find solutions as soon as possible, often frequently interjecting and demanding faster, more comprehensive solutions within unreasonable timeframes. A stress exposure training that involves a role-play scenario with high time pressure placed on the team members can help CSIRTs become more familiar with the kind of responses and internal (i.e., within-team), as well as external, stressors that can impact their teamwork.

Stress exposure training is composed of three stages: 1) explaining the importance of stress training, including identifying and coping with the specific stressors in the environment; 2) providing the team members with specially identified mental (i.e., cognitive) and behavioral coping strategies; 3) having them practice these strategies under situations that become increasingly more difficult and stressful (e.g., Ross, Szalma, & Hancock, 2004). We believe that CSIRTs will achieve these same advantages, and be able to maintain high team functioning, through the implementation of stress exposure training.

After the first stage--being informed about the stress that can be endured during incidents and the benefits of stress exposure training--the second stage consists of identifying stress-inducing events, which provides teams with the background information necessary for a facilitated discussion on how people can react to specific stressors they encounter. The emphasis in this stage is to have the trainees focus on the causes of stress and how those stress reactions can be mitigated through various techniques. Some possible techniques CSIRTs can consider include the following: skills training strategies such as overlearning (i.e., automating and simplifying complex tasks and making them less vulnerable to stress; LeBlanc, 2009), cognitive control strategies such as helping individuals recognize when task-irrelevant thoughts and emotions (e.g., worry and frustration from stress itself) arise during the training scenario and replacing them with a sense of mastery of tasks to bolster confidence in overcoming difficulties (Dweck, 2003; Keinan, 1988), attentional focus training (i.e., teaching team members to describe the conditions under which attention may be diminished during task performance, completing practice trials under difficult conditions, focus through visualizing the key tasks that need to be executed, and identify a “target point” that they could use to regain focus when distracted; Singer, Cauraugh, Murphy, Chen, & Lidor, 1991), and physiological control strategies such as relaxation training involving muscle tensing-and-relaxing exercises to reduce the physical manifestations of stress (see Murphy, 2003, for a review).

Next, during stage three, the previously discussed skills for handling stress are practiced in low-fidelity scenarios that represent the real-life situations only to a slight extent (e.g., an incident response scenario with a few analysts but no time pressure or external forces from management and clients). The purpose of the low-fidelity scenarios is to give the CSIRT trainees a chance to practice being aware of stress, using various techniques for stress reduction, and to allow time for feedback from the facilitator on how various techniques were used properly (or not). Later, low-fidelity scenarios should be replaced with high-fidelity scenarios that resemble real-life situations to a greater degree. The purpose of the high-fidelity scenarios is to provide trainees with practice in critical thinking processes under various levels of time pressure, starting with conditions that are similar to those that will be encountered during more routine incidents and then increasing that similarity over multiple training phases. Through high-fidelity scenarios, CSIRT members can become more aware not only of their own, but also their teammates’ reactions to stress and understand how they can adapt their behaviors under time pressure.

Development and implementation costs for stress exposure training are quite high due to the development of training scenarios and knowledge materials as well as the necessity to conduct the training over multiple in-person sessions. In particular, the development costs require internal and/or external subject matter experts to discuss and develop a curriculum. This requires a considerable time investment and, potentially, a relatively high financial investment if external support is used. Some costs in this area could be reduced if sufficient training simulations already exist that can be used readily or with minor adjustments. During implementation, the productivity loss for trainees is also quite high compared to other types of training. For example, stress exposure training for the military has been reported to take three full days: one day per stage of the training process (*Squad overmatch study,* 2014). While the training could possibly be cut down to one full day in CSIRTs, depending on the kinds of scenarios selected, it is important to note that the last stage of the training, during which stress increases until reaching the highest realistic level, is key for participants to transfer their training to actual workplace scenarios and, therefore, the time spent in this stage should not be significantly reduced. Despite the relatively high costs, teams that are frequently involved in high-stress situations would benefit from this kind of training and could see improved individual preparedness and team performance (Driskell et al., 1998; Driskell et al., 2001).

Another way for teams to rehearse how to react when situations do not go as planned is with **perturbation training**, which is designed to inoculate team members from falling into rigid routines and to help them adapt to stressful situations where the standard procedure will not work (Gorman, Cooke, & Amazeen, 2010). Perturbation training has been shown to lead to a 13% increase in performance in military response teams compared to teams that had not been through perturbation training (Gorman et al., 2010). To conduct this training, a series of training sessions is required.[1] Each session should match a realistic incident response situation, preferably one that requires substantial intra- and inter-team interactions. During the early sessions, teams should be afforded a more or less ideal situation (e.g., all information is accessible, all required individuals are available, all systems are functioning properly). In subsequent sessions, critical resources (e.g., personnel, equipment) should be removed or made more difficult to access. This process of disrupting the standard coordination, process timeline, and functioning of the team forces team members to adapt and become comfortable adapting to sub-optimal situations.

Similar to stress exposure training, both the development and implementation costs for perturbation training are moderate to high. The majority of development costs are due to the time required to set up realistic situations and to structure the team processes such that employees can attend the training sessions. Depending on the skills and ability levels of internal personnel available to create and structure these sessions, external support may be required, which would create an additional cost. The implementation costs are mostly due to the loss of productivity from holding multiple sessions over several weeks or months, as each training session requires several hours (Gorman et al., 2010). To limit the cost burden of perturbation training, the training scenarios could be incorporated into preexisting CSIRT training programs involving intra- and inter-team interactions. For example, if a CSIRT is practicing with a red team as a training exercise, a manager can easily implement some of the perturbation training principles to help improve the team’s adaptation abilities. In particular, the manager can temporarily remove, or delay, the rapidity with which specific indi-

[1] It is feasible that these scenarios could overlap with those created for stress exposure training, mentioned earlier, or vice versa.

viduals are able to work in order to simulate when analysts are on-call during night shifts, or driving to work, and allow the trainees to develop ways to function while help from others is not immediately accessible.

Shared mental model strategies from MR teams. Researchers have defined a shared mental model as an understanding, shared among team members, of task requirements, team interaction protocols, and member role responsibilities (Cannon-Bowers, Salas, & Converse, 1993; Peterson, Mitchell, Thompson, Burr, 2000). Several empirically supported methods exist for the development of shared mental models. We have identified two methods that are promising for the development of shared mental models among CSIRT members: guided team self-correction and the commander's intent method.

The process of **guided team self-correction**, in which teams develop their ability to assess situations through a specific framework of facilitated debriefing after training exercises, has been shown to lead to a 38% increase in teamwork processes and a 110% increase in performance (Smith-Jentsch, Cannon-Bowers, Tannenbaum, & Salas, 2008). This type of training requires experts to facilitate the ideal, or "proper," ways to assess and react to a given situation. When used in training exercises, teams are given a series of exercises and asked to work together to solve the presented problems. After each exercise is finished, a debriefing period begins as the team's actions—both successes and failures—are reviewed by the expert(s). Teams then discuss how to correct their initial process to more closely match the expert model in the future.

One specific form of this training is called Team Dimensional Training, which was developed for the U.S. Navy. When this training is integrated as a framework to existing training procedures and exercises, training scenarios are debriefed based on four dimensions (as opposed to chronological order): information exchange, communication delivery, team backup, and initiative/leadership. Trainees are provided with positive or negative feedback to cover four points for each dimension: identification of key events, identification of teamwork behaviors, a review of the solutions, and a discussion of the consequences (T. Franz, private communication, 12 August 2015). Although the average time allotted for discussing any given scenario is about 30 minutes, the initial sessions might last around an hour (Smith-Jenstch et al., 1998; T. Franz, private communication, 12 August 2015). This process of critiquing, providing feedback, and proactive planning not only provides teams an opportunity to develop their shared mental models about how to properly assess and approach various situations, but it also provides information on the team's standard processes, which can be particularly useful for recently hired team members.

The greater proportion of the investment required for this training comes from the time experts must spend creating various scenarios, documenting their resolution strategies for each scenario,[2] training the facilitators,[3] and running the debriefing period (which, as previously mentioned, could last for longer than an hour, depending on the detail of the scenario presented and the amount of alignment between the team's interpretation of how to address the situation and the expert's prescribed course of action). Thus, depending on how frequently this training is held and the availability of experts that can critique the training situations, the training requires a moderately high investment for both development and implementation.

To develop a shared (and accurate) understanding of what successful performance looks like in various situations, teams can also utilize various kinds of exercises based on the **commander's intent model** (Klein, 1993). MR teams have utilized this strategy to develop and improve aspects of decision-making skills, leadership, and shared mental models. It can be tailored to fit individual or team development needs (e.g., Klein, 1993; Crichton, Flin, & Rattray, 2000).

One version of this training, which focuses on teamwork, requires teams and their leaders to first review the same short scenario (under a few hundred words) describing a situation involving the team members. Then, all members present their assessment of the situation (including pointing out what they see as the most critical pieces of information and key courses of action), their understanding of their own role, and their understanding of other team members' roles. Following these descriptions, a trained team leader, or a subject matter expert, facilitates a discussion about discrepancies between members' assessments and those of the facilitator. This assessment and debrief period creates the necessary dialogue for correction and clarification of misperceptions between team members and their leaders (Crichton, 2009). Over time (either over a period of several weeks or multiple scenarios in one training session), the members' understanding of their tasks and the team's goals becomes automatic.

Variations of this training—"Think Like a Commander" (e.g., Shadrick, Crabb, & Lussier, 2007) and "Captain in Command" (e.g., Shadrick & Fite, 2009)—which focus on understanding situations from a leader's perspective, have been shown to increase trainees' ability to identify key pieces of information in various scenarios by over 20% (Shadrick & Fite, 2009; Shadrick & Lussier, 2004). These kinds of tactical decision-based trainings can be developed and implemented at a relatively low cost depending on the desired level of detail and the time available. Development costs can stay low by adapting preexisting training scenarios, for which case managers or subject matter experts go over the scenarios to predetermine the key pieces of information and/or best strategy.

[2] A trained Team Dimensional Training facilitator reported that this would take an employee's full-week time due to the job analysis, interviews, and scenario development and revision process (T. Franz, private communication, 12 August 2015).

[3] Smith-Jentsch and colleagues (2008) report that facilitator training lasts about two 8-hr days. Half of this period consists of classroom training where trainees listen to lectures on the guided team self-correction method, practice matching the cues in the scenarios to the ones in the expert model, critique previous sessions of videotaped facilitators, role-play portions of a debrief session, and receive feedback from others. The rest of the training period involves trainees facilitating the team dimensional training with actual teams under the supervision of the main instructor, and receiving feedback on their performance.

If more time and support are available, however, new vignettes with more detailed background information should be used to create increasingly realistic scenarios (Gonsalves, 1997). Facilitators can also increase levels of stress and difficulty by interrupting participants' thought processes, by cutting review time short, or asking questions while participants prepare their responses to the given scenario. No matter which development strategy is chosen, implementation costs are about the same, as the time required to successfully present materials (suggested 2-4 minutes per scenario; Shadrick, Lussier, & Fult, 2007), to have attendees present and discuss individual response, and then to conduct a thorough debriefing takes the same amount of time—over 1 hour (Crichton, 2001).

It is important to note that the complete training session should be conducted several times (Crichton et al., 2000), perhaps spaced out over several months, to establish strong, fully-shared mental models among the team members. This pattern of training could be particularly important for teams with higher levels of turnover because it will provide an opportunity for new members to quickly establish a shared understanding of everyone's role in various situations.

Communication recommendations from MR teams. Effective communication is required to enhance team effectiveness, especially during critical events. Moreover, exchanging information is critical for well-integrated teams and allows for the formation of adaptive teams (Cohen, Mohrman, & Mohrman, 1998; Pollack, 1998). Proper communication involves knowing what to say to whom, when, and how.

A **briefing** is a tool that requires all necessary information to be passed from one person to another while avoiding unnecessary communication, which could hinder team performance (Lee, Ha, & Seong, 2011). Briefings have been shown to reduce excessive communication by creating uniform processes that improve cohesion and allow the team to focus on the actions required to achieve team objectives (Spiker, Silverman, Tourville, & Nulimeyer, 1998). In addition, briefings that occur prior to teamwork on a given task allow each team member to be more aware of different types of information to review (e.g., possibility of different threats of which to be aware), which can increase performance (Spiker et al., 1998).

There are many different types of briefings, such as mission, decision, information, or staff briefings (see Briefing Guide, 1993, for more information). A specific type that MR teams utilize prior to specific incident response episodes is a team strategy briefing that involves establishing a clear, shared vision among all team members of what their objectives are and how to achieve them. While this technique will be discussed in more detail in the EMS teams section, team strategy briefings in military settings have been shown to augment team processes such as critical thinking, communication, coordination, and leadership by 7%, as well as facilitate the establishment of shared mental models by improving their development by about 33% (Dalenberg et al., 2009). Based on our personal interviews, some cybersecurity communities conduct 30-minute strategy briefings prior to high-profile incidents where collaboration among several teams is required for incident response. One member from each team is required to attend these briefings and relay the information about incident severity and status from the briefing to his or her respective team. Conducting team strategy briefings with members from the same team can also improve the incident response process by allowing the members to set goals and determine teamwork requirements for effective incident response. Briefings can be implemented with very low development and implementation costs as they often require only a few minutes for a team to identify main goals and define each individual's responsibilities. The largest investment would be getting buy-in from management, leadership, and team members so that they consistently enforce the use of briefings during regular work tasks. At a somewhat minimal additional cost, this kind of behavior can be integrated into more formal teamwork training through role-play (see Awad et al., 2005, for an example).

Trust recommendations from MR teams. One of the most important factors for team success is trust between team members (Blair & Hanna, 2009). Trust helps define the relationships between team members, specifically whether they believe they can rely on each other in risky or dangerous situations (Mayer, Davis, & Schoorman, 1995). Unlike previously discussed recommendations for improving team effectiveness, trust, as an emotional response to a person or a given situation, cannot be as easily "trained" as communication, adaptation, or shared mental models. However, this does not negate the importance of supporting the development of trust within teams.

Although its impact is indirect, trust has been found in numerous studies to be a key component of team processes that lead to high effectiveness and performance (e.g., Kiffin-Petersen, 2004; Costa, 2003; Dirks & Ferrin, 2001). For example, Wildman and colleagues (2012) found that when team members were able to trust one another, there was a decrease in conflict and an increase in information sharing and cooperation. Trust facilitates these important team processes and serves as the foundation for good team performance and team member satisfaction (Priest, Stagl, Klein, & Salas, 2006; Wildman et al., 2012).

Given the reliance on other team members during dangerous missions, the military may provide the ideal example on the importance of trust in fellow team members (Blair & Hanna, 2009; Olison, 2012). In military teams, long-term trust can be established by (a) using word-of-mouth praise to build members' reputations of team members, (b) openly reflecting on levels of expertise possessed by team members, (c) emphasizing similarities among team members with regard to professional or personal background, and (d) fostering team satisfaction (Blair & Hanna, 2009). Trust can also be built by discussing each member's professional strengths and the areas where they would like support from other team members (Holton, 2001). These kinds of behaviors help establish feelings of similarity (see the similarity-attraction hypothesis for more information; Blankenship, Hnat, Hess, & Brown, 1984; Novak & Lerner, 1968) and perceived safety within the team, which both elevate levels of trust between team members (Debra, Weick, & Kramer, 1995).

Team norms, often set by leaders, can also influence levels of trust within teams (Dickson, Smith, Grojean, & Ehrhart, 2001).[4] During training and other learning exercises, CSIRT leaders can develop trust by asking individual team members to provide their own opinions on different issues or situations to establish a sense that everyone's opinion is valued and appreciated. Along those lines, encouraging the open discussion of mistakes can make teams twice as likely to detect errors compared to teams without such trusting and supportive team environments (Edmondson, 2003). Other techniques that can promote trust in a team include providing a well-defined task (i.e., a small, concrete task) to each team member to promote a greater sense of control, informing members about impending events to increase certainty, and creating a friendly, positive climate within the team to promote interpersonal relations (Hedlund, Börjesson, & Österberg, 2015). Furthermore, having clarity of team goals and team member roles can also improve trust within a team (Klein, Ziegart, Knight, & Xiao, 2006). Since these strategies are most effective in the form of established norms—patterns that occur regularly and frequently within a team's work processes—utilizing these behaviors only one time will not likely produce the desired results. Therefore, it is important to have a way to enforce the sustained use of these behaviors, which can be done through change management principles (see the Change Management section in the General Discussion).

The costs of utilizing the aforementioned trust-building strategies can be difficult to gauge because they depend heavily on how the leader of each team behaves, manages discussions among team members, and maintains trust-enforcing work norms for his or her group. However, in general, the typical kinds of actions that can be taken to develop team trust are rather simple and require minimal time and financial investment (e.g., find commonalities between team members, create an open environment through asking others' opinions).

MR teams summary. Due to the vital role United States MR teams play in military operations across the globe, a vast amount of research has been conducted on understanding and improving MR teamwork. From this body of research, we were able to extract a number of training programs CSIRTs can modify to improve their ability to adapt (e.g., critical thinking training, stress exposure training, and perturbation training), to develop shared mental models (e.g., guided team self-correction and the commander's intent method), to communicate (e.g., briefing), and to employ trust-building behaviors. To help CSIRTs maximize their investment, a cost-effectiveness breakdown and discussion of when to favor a specific recommendation is presented in the General Discussion to this appendix (see also Table F.1 and Table F.2 below).

F.3.2 EMERGENCY MEDICAL SERVICE TEAMS

Emergency Medical Service (EMS) teams provide a range of emergency health services such as offering advice on emergency call-in lines, treating injured individuals at emergency scenes, passing along health and risk communication to other health professionals, handing off patients to other teams, conducting traumatic care in hospital emergency departments, and creating documentation of treatment (USDHHS, 2005; SBCCOM, 2003; Schottke, 2010). Pre-hospital emergency responders may be composed of emergency dispatchers, paramedics, ambulance drivers, helicopter pilots, and other personnel (Schottke, 2010), whereas hospital-based emergency teams may additionally include nurses and physicians (Fernandez, Kozlowski, Shapiro, & Salas, 2008). In addition, EMS teams can take different forms, such as rapid response teams (Leach & Mayo, 2013), combat trauma care teams (Brady, 2011) and forward surgical teams (Brady, 2011).

Pre-hospital EMS teams can handle cases that vary in their level of severity. As examples, a small-scale situation could be a car accident requiring paramedic assistance whereas a large-scale response could be a natural disaster or a terrorist attack involving EMS teams from a variety of agencies and hospitals. The ultimate goal of both pre-hospital and hospital-based EMS teams is safe handling of patients and mitigation of adverse events (Kohn, Corrigan, & Donaldson, 1999).

Although CSIRTs and EMS teams differ with regard to the origin of the incidents they handle (IT systems vs. humans) and the physical work environments in which they operate (office buildings vs. emergency scenes), in most cases the core elements of their roles and the characteristics of the problems they face remain the same. That is, they both operate in complex, stressful, changing, collaborative environments. As such, the teamwork skills required for both CSIRTs and EMS teams are similar.

The role of adaptation in CSIRTs has already been discussed previously, and recommendations from MR teams have been put forward. A vast amount of research exists on how to improve team adaptation in EMS teams as well. Healthcare organizations utilize specialized teamwork training programs[5] that target a variety of key areas for improved adaptation: team leadership, situation monitoring, mutual support, and communication, as well as teamwork skills like knowledge of team processes, team attitudes (e.g., mutual trust) and team performance

[4] In CSIRTs and military teams that create ad hoc teams to handle incidents once they occur, trust must be established quickly. This kind of initial trust is called "swift trust" (Mishra, 1996) and can be established in several ways. One method that has been used with newly formed military teams is to create a team name or motto in order to establish a shared identity, which can quickly lead to higher levels of trust (about 7% in Adams, Waldherr, Sartori, & Thomson, 2007). Another method is to give a brief overview of each new team member's credentials or achievements so members believe in their team members' competence in completed required work (Blair & Hanna, 2009).

[5] These training programs are crew resource management (CRM) training and the Team Strategies and Tools to Enhance Performance and Patient Safety (TeamSTEPPS), which was developed from CRM. For more information on these programs, see Alonso et al., 2006; Baker, Gustafson, Beaubien, Salas, and Barach, 2005; Fernandez et al., 2008; King et al., 2008; Salas et al., 2008; O'Connor et al., 2008; Weaver et al., 2010; Weaver, Rosen, Shekelle, Wachter, & Provonost, 2013.

TABLE F.1: COST-EFFECTIVENESS INFORMATION FOR RECOMMENDED STRATEGIES

STRATEGY	DEFINITION	EFFECTIVENESS (BENEFIT)	DEVELOPMENT COST	IMPLEMENTATION COST	SELECTED REFERENCES
Critical Thinking Training	A training program that aims to develop one's ability "to systematically assess a situation, integrate different observations into a coherent story, identify uncertainties and justify assumptions, and come up with contingency plans" (van den Bosch, Helsdingen, & de Beer, 2004, p. 9)	27% - 41% improvement in the situation assessment 58% improvement in problem-related observations 41% improvement in alternative solution generation 35% to 79% agreement among subject matter experts in the respective decisions (Cohen, Freeman, et al., 1998)	Moderate	Moderate	van den Bosch, Helsdingen, & de Beer (2004); Cohen, Freeman, et al. (1998)

Checklist	A list of required actions (both task and interpersonal), as well as teamwork-related behaviors, that should be performed during various situations (e.g., Lingard et al., 2008; Taylor, Hepworth, Buerhaus, Dittus, & Speroff, 2007)	100% reduction in adverse events (Leonard et al., 2004)
		16% less turnover (Leonard et al., 2004)
		19% more employee satisfaction (Leonard et al., 2004)
		64% reduction in communication failures (Lingard et al., 2008)
			Moderate	Moderate	Harden (2013);
					Verdaasdonk et al. (2009);
					Hefford & Blick (2012)

SBAR Handoff Protocol	A protocol that stand for Situation, Background, Assessment, and Recommendation, and is used to prevent communication breakdowns among team members by conveying relevant information and creating shared mental models (Pham et al., 2012; Cziraki et al., 2008; Pettker et al., 2009; Riesenberg, Leitzch, & Little, 2009; Velji et al., 2008)	65% decrease in adverse events (Deering et al., 2011)
		53% to 89% improvement in patient handling processes (Haig et al., 2006)
		40% decrease in adverse drug events (Haig et al., 2006)
		12% decrease in handoff times (Riesenberg, Leitzsch, & Little, 2009)
			Low	Moderate	Riesenberg, Leitzch, & Little (2009);
					Velji et al. (2008);
					Haig et al. (2006)

Pre-brief (including team strategy brief)	Short discussion before or during a work event that involves establishing a clear, shared vision among all team members of what their objectives are and how to achieve them (e.g., Briefing Guide, 1987)	7% improvement in team processes like critical thinking, communication, coordination and leadership 33% further development in shared mental models (Dalenberg, Vogelaar, & Beersma, 2009) 64% decrease in communication failures (Lingard et al., 2008) 27%-125% improvement in team communication scores (Awad et al., 2005)	Low	Moderate	Awad et al. (2005); Tybinski et al. (2012)

Note: Development and implementation costs were each rated by industrial-organizational psychology graduate students on a 1 (Low) to 3 (High) scale via consensus after the raters consulted available references that listed the costs (in terms of money and/or time) associated with aspects of the strategies.

TABLE F.1: COST-EFFECTIVENESS INFORMATION FOR RECOMMENDED STRATEGIES (CONTINUED)

STRATEGY	DEFINITION	EFFECTIVENESS (BENEFIT)	DEVELOPMENT COST	IMPLEMENTATION COST	SELECTED REFERENCES

Debriefing / After-action Review (after each key learning opportunity)	Teams take time to evaluate team processes and actions, including: description of the event, the category of the event, a list of the communication tools or methods used, and things the team did well and could improve (Turner, 2012)	20-25% improvement in teamwork performance (Tannenbaum & Cerasoli, 2012)
		10% decrease in work delays
		5% decrease in handoff issues
		almost 20% increase in overall work quality (as reflected in case scores) (Wolf et al., 2010)
			Moderate	Moderate	Popper & Lipshitz (2000);
					Orlansky, Taylor, Levine, & Honing (1997);
					Arora et al. (2012);
					Tannenbaum & Cerasoli (2012)

Stress Exposure Training	A training program designed to foster stress coping by familiarizing team members with dynamic and high-stress environments and teaching them the skills to maintain effective team functioning and task performance in such environments (Driskell et al., 1998)	18% improvement in team performance (Driskell et al. 1998; Driskell et al., 2001)	Moderate	Moderate	Driskell et al. (1998); Driskell et al. (2001)
Perturbation Training	A training program that inoculates team members from falling into rigid routines and to help them adapt to stressful situations where the standard procedure will not work (Gorman et al., 2010)	13% increase in performance (Gorman, et al., 2010)	Moderate	Moderate	Gorman, Amazeen, & Cook (2010)

Cross-Training	A training program that allows team members to obtain knowledge of other team members' roles (interpositional knowledge), which will allow teams to be prepared for coordinating actions effectively by understanding each other's needs (Salas et al., Nichols, & Driskell, 2007; Volpe, Cannon-Bowers, Salas, & Spector, 1996)	33% increase in team members' understanding of their own roles as well as the roles of other team members (Espevik et al., 2011)	Moderate	Moderate	Salas et al., Nichols, & Driskell (2007);
					Volpe, Cannon-Bowers, Salas, & Spector (1996);
					Espevik et al. (2011)

Note: Development and implementation costs were each rated by industrial-organizational psychology graduate students on a 1 (Low) to 3 (High) scale via consensus after the raters consulted available references that listed the costs (in terms of money and/or time) associated with aspects of the strategies.

TABLE F.1: COST-EFFECTIVENESS INFORMATION FOR RECOMMENDED STRATEGIES(CONTINUED)

STRATEGY	DEFINITION	EFFECTIVENESS (BENEFIT)	DEVELOPMENT COST	IMPLEMENTATION COST	SELECTED REFERENCES
Guided team self-correction	A training program emphasizing the comparison and emulation of experts' incident response processes (Smith-Jentsch et al., 2008)	38% increase in teamwork processes 110% increase in performance (Smith-Jentsch et al., 2008)	Moderate	Moderate	Smith-Jentsch et al. (2008)
CUS	The CUS protocol (meaning: I am Concerned!, I am Uncomfortable!, This is a Safety issue!) improves communication during stressful times by increasing clarity and awareness among team members of a possible problem, resulting in improved mutual support and understanding of the level of concern being raised	20% improvement in leadership scores 18% more situation monitoring 16% more mutual support 53% improved communication 18% improved overall teamwork 26% decrease in average time (in minutes) to transition from various work tasks (Capella et al., 2010)	Moderate	Moderate	Maguire et al. (2015); Clapper (2013)

Commander's intent / Think like a Commander	Training programs where the teams and their leaders review the same short scenario (under a few hundred words) and then have all members present their assessment of the situation (including pointing out what they see as the most critical pieces of information and key courses of action), their understanding of their own role, and their understanding of other team members' roles (Crichton, 2009)	20% increase in the ability to identify key pieces of information (Shadrick et al., 2007a; Shadrick & Fite, 2009)	Moderate	Low	Crichton (2009);
					Shadrick et al. (2007a);
					Shadrick & Fite (2009)

Trust building behaviors	Behaviors that create a sense of support, safety, or similarity, like praising team members' expertise, determining professional or personal similarities between team members (Blair & Hanna, 2009), and discussing each member's personal strengths and weaknesses (Holton, 2001)	Twice as many errors detected (Edmondson, 2003)	Low	Moderate	Adams et al. (2007);
					Hedlund (2015);
					Klein, Ziegart, Knight, & Xiao (2006)

Note: Development and implementation costs were each rated by industrial-organizational psychology graduate students on a 1 (Low) to 3 (High) scale via consensus after the raters consulted available references that listed the costs (in terms of money and/or time) associated with aspects of the strategies.

TABLE F.2: SUMMARY OF RECOMMENDATIONS BASED ON AREAS TO IMPROVE AND RELATIVE DEVELOPMENT AND IMPLEMENTATION COSTS

RECOMMENDATIONS			
AREA TO IMPROVE/ ADDRESS	**LOWER INVESTMENT**	**HIGHER INVESTMENT**	**MOST COST-EFFECTIVE STRATEGIES**
Adaptation	• Critical thinking training • Perturbation training	• Stress exposure training	• Critical thinking training
Shared Mental Model	• Cross-training (positional clarification, positional modeling) • Commander's intent	• Guided team self-correction • Cross-training (positional rotation)	• Cross-training (positional clarification)
Communication	• Pre-briefs • Checklists (paper, normal situations) • After-action review	• Checklists (electronic, variety of situations) • Situation, Background, Assessment, and Recommendation (SBAR)	• Checklists (paper, normal situations) • Situation, Background, Assessment, and Recommendation (SBAR)
Trust	• Developing trust norms • Encourage open discussion of mistakes • Ask for others' opinions • Clarity of goal and roles • Friendly team climate • Find similarities amongst team members	• I am Concerned!, I am Uncomfortable!, This is a Safety issue! (CUS)	• Developing trust norms

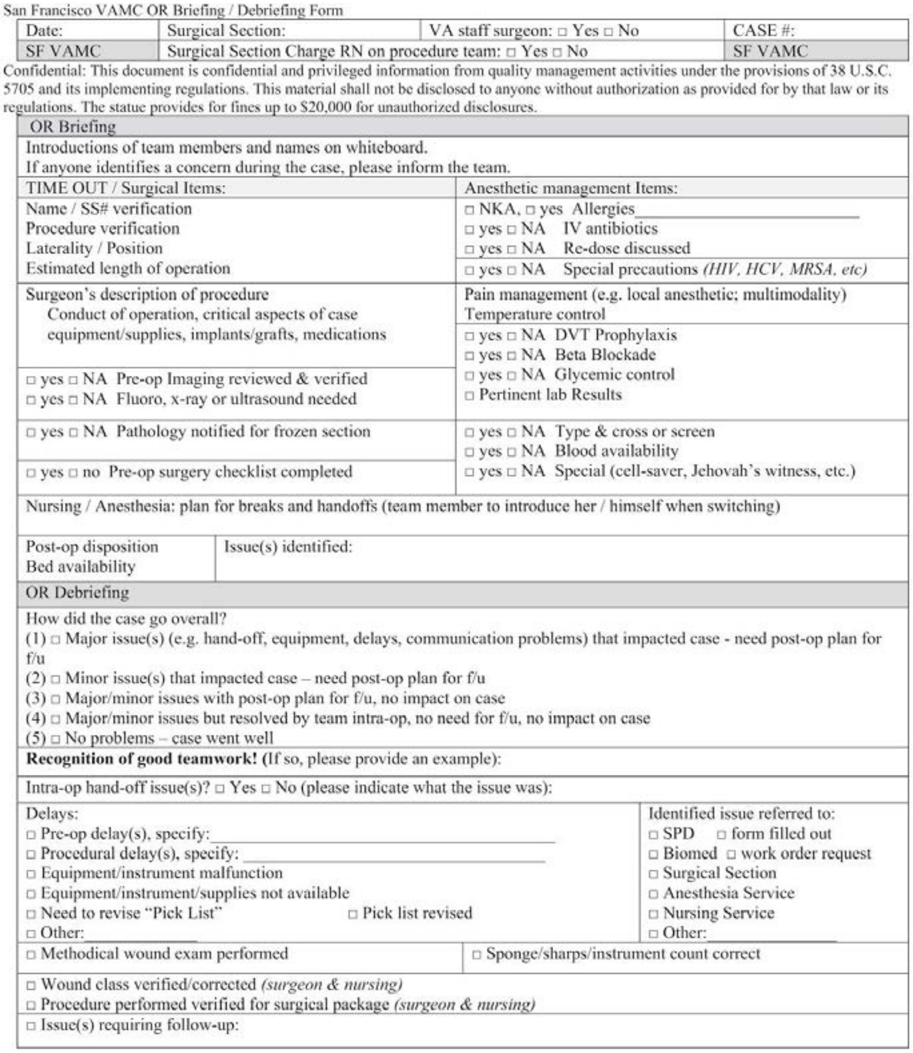
(Alonso et al., 2006). For the EMS section, we will focus on several of the specific strategies used in these training programs that have been researched independently and can easily be adapted to CSIRTs. Namely, we will focus on enhancing clear communication and improving trust through team-based leadership.

Communication strategies from EMS teams. Communication is critical to the success of EMS teams. A recent review of medical teamwork research identified communication as the most prominent teamwork component (Dietz et al., 2014) because communication breakdowns among healthcare providers have been found to be the number one cause of medical error--accounting for nearly 70% of the errors (Kohn et al., 1999; Morey, Simon, Jay, & Rice, 2003; Sutcliffe, Lewton, & Rosenthal, 2004).

Most communication breakdowns in healthcare occur during patient handoffs. Handoffs are also a process of major concern for CSIRTs. In fact, Hewlett-Packard (2014) recently reported that the most cyber incident handling errors occur during shift changes and handoffs. Research on patient handoffs has found that EMS teams that communicate effectively during handoffs can detect medical errors and prevent adverse events as the person taking over the patient reviews the information with a novel perspective (Hall, Rudolf, & Cao, 2006; Patterson, Roth, Woods, Chow, & Gomes, 2004). Several key strategies have been identified as ways to improve communication during handoffs: checklists, communication protocols, and briefs/pre-briefs.

Checklists ensure that teams recognize and deal with unexpected problems that may come up in complex environments (Gawande, 2009). They are relatively consistent in their effectiveness in improving outcomes. For example, researchers have found that checklists reduced adverse events by up to 100%, reduced employee turnover by 16%, and improved operating room employee satisfaction by 19% (Leonard, Graham, & Bonacum, 2004). In addition, overall communication failures (e.g., untimely information provision, missing information) were reduced by 64% (Lingard et al., 2008). Despite the effectiveness of integrating checklists into regular work procedures, publications in the medical community (e.g., Gawande, 2009), as well as our interviews with several CSIRTs across different companies, have shown that team members who are required to use checklists consider the checklists a burden and often show resistance to using them. Luckily, change management research has uncovered several barriers and possible solutions for overcoming these barriers when trying to implement procedural changes, which we discuss later in this appendix.

Although the vast majority of CSIRTs already integrate various kinds of checklists into their work processes, the major difference, and key element, of medical checklists that distinguish them from those used in most CSIRTs is that EMS teams often incorporate interpersonal actions alongside main tasks so that teamwork principles and communication are also included. Figure F.1 is an example operating room checklist, and it identifies some of these interpersonal items: "surgeon's description of procedure," "plans for breaks and handoff (team member to introduce her or himself when switching)," "recognition of good teamwork," and "handoff issues." For CSIRTs, similar items could reference the quality of the manager's or team lead's descriptions of the incident response task that needs to be done, whether or not team members or leaders provide positive feedback on good coordina-



San Francisco VAMC OR Briefing / Debriefing Form

Date:	Surgical Section:	VA staff surgeon: □ Yes □ No	CASE #:
SF VAMC	Surgical Section Charge RN on procedure team: □ Yes □ No		SF VAMC

Confidential: This document is confidential and privileged information from quality management activities under the provisions of 38 U.S.C. 5705 and its implementing regulations. This material shall not be disclosed to anyone without authorization as provided for by that law or its regulations. The statue provides for fines up to $20,000 for unauthorized disclosures.

OR Briefing

Introductions of team members and names on whiteboard.
If anyone identifies a concern during the case, please inform the team.

TIME OUT / Surgical Items:	Anesthetic management Items:
Name / SS# verification Procedure verification Laterality / Position Estimated length of operation	□ NKA, □ yes Allergies____________________ □ yes □ NA IV antibiotics □ yes □ NA Re-dose discussed □ yes □ NA Special precautions *(HIV, HCV, MRSA, etc)*
Surgeon's description of procedure Conduct of operation, critical aspects of case equipment/supplies, implants/grafts, medications	Pain management (e.g. local anesthetic; multimodality) Temperature control
□ yes □ NA Pre-op Imaging reviewed & verified □ yes □ NA Fluoro, x-ray or ultrasound needed	□ yes □ NA DVT Prophylaxis □ yes □ NA Beta Blockade □ yes □ NA Glycemic control □ Pertinent lab Results
□ yes □ NA Pathology notified for frozen section □ yes □ no Pre-op surgery checklist completed	□ yes □ NA Type & cross or screen □ yes □ NA Blood availability □ yes □ NA Special (cell-saver, Jehovah's witness, etc.)

Nursing / Anesthesia: plan for breaks and handoffs (team member to introduce her / himself when switching)

Post-op disposition Bed availability	Issue(s) identified:

OR Debriefing

How did the case go overall?
(1) □ Major issue(s) (e.g. hand-off, equipment, delays, communication problems) that impacted case - need post-op plan for f/u
(2) □ Minor issue(s) that impacted case – need post-op plan for f/u
(3) □ Major/minor issues with post-op plan for f/u, no impact on case
(4) □ Major/minor issues but resolved by team intra-op, no need for f/u, no impact on case
(5) □ No problems – case went well

Recognition of good teamwork! (If so, please provide an example):

Intra-op hand-off issue(s)? □ Yes □ No (please indicate what the issue was):

Delays:	Identified issue referred to:
□ Pre-op delay(s), specify:____________________	□ SPD □ form filled out
□ Procedural delay(s), specify: ____________________	□ Biomed □ work order request
□ Equipment/instrument malfunction	□ Surgical Section
□ Equipment/instrument/supplies not available	□ Anesthesia Service
□ Need to revise "Pick List" □ Pick list revised	□ Nursing Service
□ Other:__________	□ Other:__________

□ Methodical wound exam performed	□ Sponge/sharps/instrument count correct

□ Wound class verified/corrected *(surgeon & nursing)*
□ Procedure performed verified for surgical package *(surgeon & nursing)*

□ Issue(s) requiring follow-up:

Figure F.1. Example EMS checklist
Note: From "The efficacy of medical team training: improved team performance and decreased operating room delays: A detailed analysis of 4863 cases," by F.A. Wolf, L.W. Way, and L. Stewart, 2010, Annals of Surgery, 252(3), p. 478. Copyright 2010 by Wolters Kluwer Health, Inc. Reprinted with permission.

tion and collaboration skills, whether or not all required information was provided during handoff or if new shifts need to go back and find more information to properly continue the work on a particular incident, and if next steps have been clearly outlined and the receiving team (i.e., the team that takes over the new shift) confirms understanding of their role expectations and next steps.

EMS teams often add checklists into teamwork training sessions to act as a tool in identifying the cause of communication breakdowns (as opposed to checking procedural knowledge). For this kind of exercise, trainees with different roles (e.g., surgeons, nurses, anesthesiologists) independently create checklists of work steps in patient care and note the tasks that are assigned to them in each step. These lists are then reviewed as a group to determine whether the team members have a shared understanding of communication points and responsibilities (e.g., Lingard et al., 2008; Taylor, Hepworth, Buerhaus, Dittus, & Speroff, 2007). Any discrepancies can then be addressed through debriefings prior to patient treatments and also during future training sessions.

CSIRTs can take a similar approach by first identifying the causes of communication breakdowns within their teams through multiple analysts (ideally at different levels) creating checklists of their understanding of the following: incident response processes (e.g., triage, escalation), information they must share during these processes, with whom they must share that information, any complications that tend to occur during these processes and interactions, and their individual roles throughout the processes. Those checklists can then be compared to one another and to lists created by subject matter experts. Discrepancies among the lists can indicate the causes of communication errors and can be addressed to create methods for overcoming those problems as well as to establish shared mental models around what the expected actions are for those individuals involved in a particular situation or response.

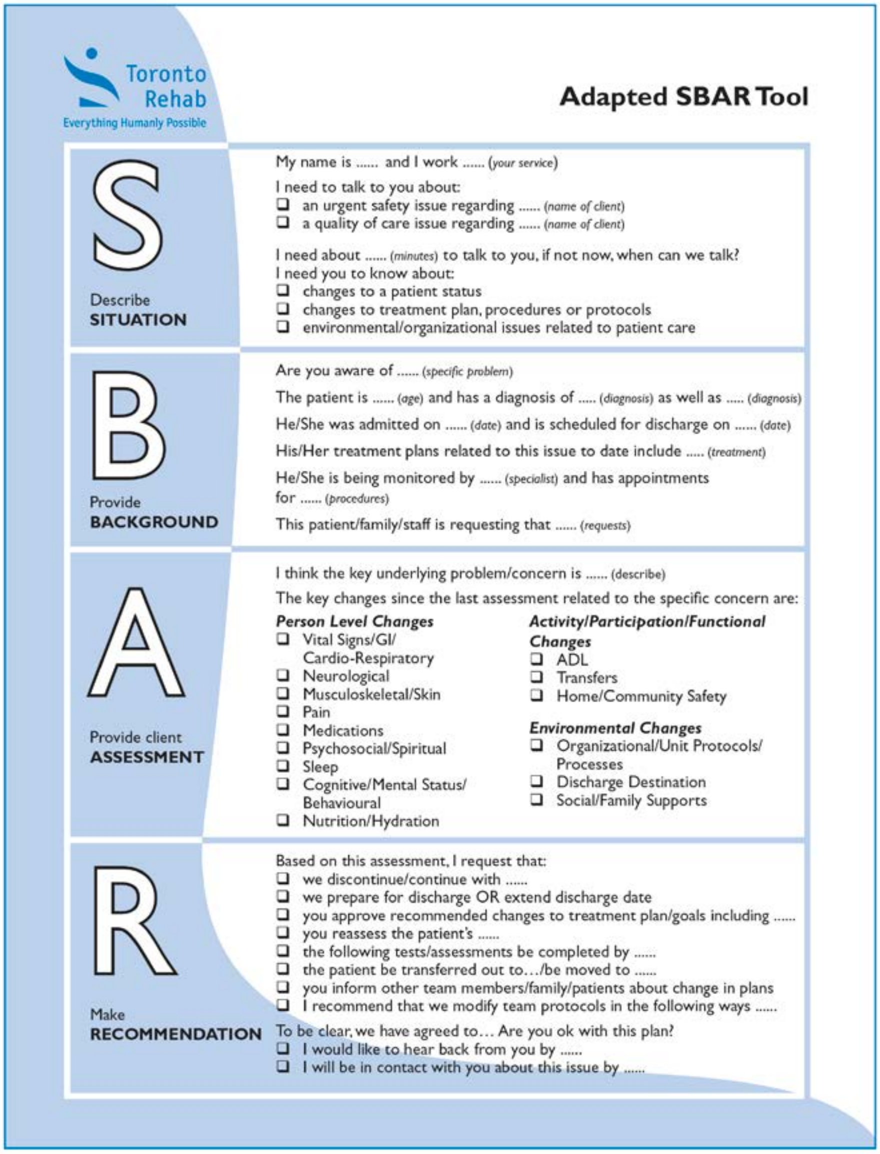
In addition, these kinds of exercises would create their own deliverables because the final checklists can be kept and used for future reference about how to handle particular situations. Although many general checklists for CSIRT processes already exist, research in the medical field has found that the most effective checklists are adapted to "fit the culture, workflow, and practice patterns of the office setting where they will be implemented...attempting to impose a [generic checklist] in an office setting without customization will only cause resistance" (Harden, 2013, p. 3). Thus, taking the time to have internal teams discuss, design, and finalize the procedures they find most relevant and important for certain situations is crucial.

Although a checklist that is already in use can be viewed as a "simple, cheap, effective, and transmissible" tool (Gawande, 2009, p. 97), proper development and implementation of this tool actually requires a fair amount of resources. In one publication, Verdaasdonk and colleagues (2009) cover, in great depth, recommendations for the design and implementation of checklists. Recommendations for design include details such as the font for heading and body texts, and recommendations for implementation include 14 steps ranging from defining the purpose of the checklist to getting the checklist reapproved by supervisors. Thus, depending on the quantity of checklists created and the complexity of the processes being documented, the development and implementation of checklists can be more costly, than what might have been initially expected, due to the time investment of personnel. However, it is important to note that checklists for routine procedures can often be more general, and required actions can be listed without needing to be in sequential order, whereas checklists for atypical or emergency situations must usually adhere to stricter standards of detail and procedural steps (Verdaasdonk et al., 2009). In addition, either electronic or paper versions of a checklist can be used, but these versions vary in both benefits and costs. While paper versions are often easier to read and cheaper to produce, electronic versions can be updated more easily and can be integrated with software to collect and transfer data more quickly (Verdaasdonk et al., 2009).

Development and implementation costs of checklists, however, are somewhat offset by the relatively inexpensive cost of subsequent use of the checklists. Previous studies on surgical teams found checklists had no negative impact on team productivity and negligible impact on the time to perform required tasks (Hefford & Blick, 2012), and operating room teams that were familiar with a given checklist were able to complete it in about one minute (Harden, 2013). However, as previously mentioned, the successful implementation of checklists can be fraught with difficulty.

One of the biggest complications associated with adopting checklists is ensuring they are used in a consistent and accurate manner. Research in EMS teams has shown that this is necessary to yield the positive impact of the checklists (Bergs et al., 2014). One CSIRT interviewee stated that although checklists are used in training to review what new people have missed in a process, "[t]he discipline in doing that is not always there." This issue is not unique to the cybersecurity domain. One study found that even though checklists were completed 90% of the time when required, only 61% of the items included on the checklists were actually performed (Fourcade, Blache, Grenier, Bourgain, & Minvielle, 2011), thus degrading the effectiveness of the checklist. Gawande (2009) suggests that medical professionals are reluctant to use the checklists because they are seen as a tedious paperwork requirement, and, for those with decision authority, as a tool that automates actions and, thus, takes away the decision power. Based on the change management literature, one way to attend to such resistance is the identification of key change agents and leaders within the organization who are willing to support and reinforce the proper use of new work procedures (van Dijk & van Dick, 2009). Several hospitals report having taken this approach--change agents called "champions," who are staff from various departments (e.g., administration, surgery, anesthesiology, and nursing), coordinate and encourage the use of the newly developed checklists (Hefford & Blick, 2012). These efforts can require up to 40 hours of work time, spread over a one-year period, for each change agent.

It should also be noted that checklist use in medical teams is effective when there are specific protocols and actions that must be followed in order to successfully complete a task (e.g., Harden, 2013; Hayes, 2012). Due to the frequent flexibility necessary in CSIRT work, it is reasonable to suggest that checklists would be most effective (and more easily implemented) in normal work



Toronto Rehab
Everything Humanly Possible

Adapted SBAR Tool

S
Describe
SITUATION

My name is ...... and I work ...... *(your service)*
I need to talk to you about:
❑ an urgent safety issue regarding ...... *(name of client)*
❑ a quality of care issue regarding ...... *(name of client)*

I need about ...... *(minutes)* to talk to you, if not now, when can we talk?
I need you to know about:
❑ changes to a patient status
❑ changes to treatment plan, procedures or protocols
❑ environmental/organizational issues related to patient care

B
Provide
BACKGROUND

Are you aware of ...... *(specific problem)*
The patient is ...... *(age)* and has a diagnosis of ..... *(diagnosis)* as well as ..... *(diagnosis)*
He/She was admitted on ...... *(date)* and is scheduled for discharge on ...... *(date)*
His/Her treatment plans related to this issue to date include ..... *(treatment)*
He/She is being monitored by ...... *(specialist)* and has appointments
for ...... *(procedures)*
This patient/family/staff is requesting that ...... *(requests)*

A
Provide client
ASSESSMENT

I think the key underlying problem/concern is ...... (describe)
The key changes since the last assessment related to the specific concern are:

Person Level Changes
❑ Vital Signs/GI/
Cardio-Respiratory
❑ Neurological
❑ Musculoskeletal/Skin
❑ Pain
❑ Medications
❑ Psychosocial/Spiritual
❑ Sleep
❑ Cognitive/Mental Status/
Behavioural
❑ Nutrition/Hydration

Activity/Participation/Functional Changes
❑ ADL
❑ Transfers
❑ Home/Community Safety

Environmental Changes
❑ Organizational/Unit Protocols/
Processes
❑ Discharge Destination
❑ Social/Family Supports

R
Make
RECOMMENDATION

Based on this assessment, I request that:
❑ we discontinue/continue with ......
❑ we prepare for discharge OR extend discharge date
❑ you approve recommended changes to treatment plan/goals including ......
❑ you reassess the patient's ......
❑ the following tests/assessments be completed by ......
❑ the patient be transferred out to…/be moved to ......
❑ you inform other team members/family/patients about change in plans
❑ I recommend that we modify team protocols in the following ways ......
To be clear, we have agreed to… Are you ok with this plan?
❑ I would like to hear back from you by ......
❑ I will be in contact with you about this issue by ......

Figure F.2a. Sample customized SBAR tool
Note: From "SBAR: A shared structure for effective team communication: 2nd Edition," by B. Trentham, A., Andreoli, N. Boaro, K. Velji and C. Fancott, 2010, p.4. Copyright 2010 by Toronto Rehabilitation Institute. Reprinted with permission.

situations where there is relatively low time pressure or stress; for example, when there are only low-severity incidents occurring. Adding checklists to regular work practices first might result in less negative initial impacts on performance and adoption than attempting to add checklist requirements to situations where people are rushing to achieve a result or solve an issue. This should be fairly easy because many of the analysts to whom we have spoken suggest that these periods of handling low-severity incidents account for roughly 80% of their response duties.

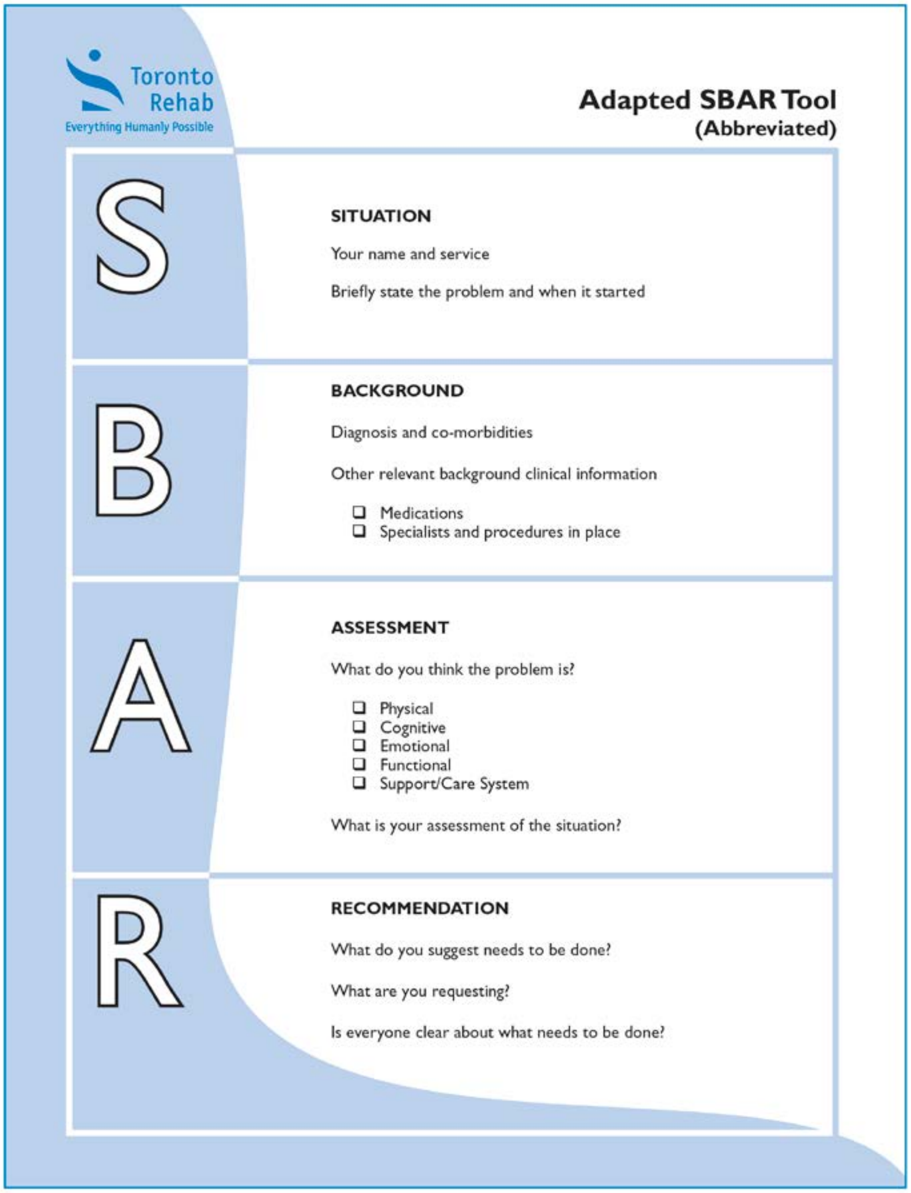
The second communication tool from EMS teams, **handoff protocols**, are also emphasized through training programs and used on a constant basis. There are many mnemonic handoff protocols used in medical care, including SBAR (Situation, Background, Assessment, and Recommendation), SHARED (Situation, History, Assessment, Risks, Events, and Documentation), MIST (Mechanism of injury, Injuries sustained, Signs, Treatment initiated), and SOAP (Subjective information, Objective information, Assessment, Plan) (see Riesenberg, Leitzch, & Little, 2009 for a review). A systematic review of articles published between 1987 and 2008, which focused on handoff protocols, identified 24 mnemonics. SBAR was cited in 69.6% of these articles reviewed. This clearly indicates that SBAR is the mnemonic that has been most widely studied. Further, SBAR has been incorporated into nationwide medical teamwork training programs (Alonso et al., 2006). Thus, we focus on SBAR as a recommendation to improve communication within CSIRTs.

To follow the SBAR protocol, the individual initiating the handoff concisely summarizes and describes the situation ("S") to the incoming team member(s). In a CSIRT, this may include information about the analyst(s) currently in charge, their position and the status of the event or incident being handed off (e.g., whether the event has been categorized as an incident, at what stage the team is in the incident response process). Next, the individual initiating the handoff shares the background ("B") information that contributed to the situation taking place. For a cybersecurity event or incident, background information can include details such as when the event was detected, what actions have been taken to investigate, what information has been obtained (or not clarified) by those actions, and the names and contact information of the individuals who have already been notified, or are "in the loop," about this event. Next, the individual initiating the handoff provides his or her assessment ("A") of the situation to the incoming team member. For a CSIRT analyst, this could be a formal classification of the event or incident along with the rationale for that classification. Finally, the individual initiating the handoff offers a recommendation ("R") for the most appropriate next steps and initiates a dialogue with the incoming team member to address any questions he or she may have before starting his or her work. In a CSIRT, the outgoing analyst could explain what further steps his or her team was planning to take but unable to conduct, indicate whether or not the incident needs to be escalated to a higher level, make suggestions as to who could be involved in resolving the incident, and then end with asking for agreement or questions from the incoming team member(s).

The use of SBAR has been shown to reduce mortality in medical institutions by standardizing the interactions among team members, helping them to convey relevant information, and creating a shared mental model of patient treatment (Cziraki et al., 2008; Pettker et al., 2009; Pham et al., 2012; Riesenberg et al., 2009; Velji et al., 2008). Researchers have found that using protocols, such as SBAR, to fix communication issues improved a number of patient outcomes, including lowering medication and transfusion errors by 65% (Deering et al., 2011), reducing adverse drug events by 40% (Haig, Sutton, & Whittington, 2006), and improving medication reconciliation[6] at patient admission by 16% and at discharge by 36% (Haig et al., 2006).

Although cybersecurity research acknowledges the importance of handoff processes, provides detailed handoff frameworks (e.g., Alberts, Dorofee, Killcrece, Ruefle, & Zajicek, 2004), and demonstrates that elements of SBAR are very similar to what most CSIRTs use when handing off information to others, SBAR still provides two new benefits. First, SBAR emphasizes the communications that occur through interpersonal team interactions. It can be used not only to create an ad hoc script for what information should be communicated verbally but also as a structure for communicating any written records. Second, SBAR allows individuals taking over a situation to understand the thought processes of the original analyst(s) and clarifies next steps to close the ticket or escalate; in other words, it helps team members develop shared mental models. An additional advantage of SBAR is that it can be integrated with checklists. Figure F.2a shows a customized SBAR tool from a Canadian rehabilitation facility. As can be seen in the figure, instead of listing tasks that need to be accomplished, a script is presented that individuals can follow not only to collect the necessary information from others but also to know in advance the kinds of information they will need to tell others in the event of a handover or event complication.

SBAR protocol is generally associated with very low development costs because, due to its extensive use in medical organizations, many SBAR models already exist (see Figure 2b for an example). Although these templates were developed for medical use, they can readily be adapted for use by a CSIRT interested in using this kind of protocol. Depending on the complexity of communication interactions (e.g., variability of communication content, number of members in communication with each other), more time might be required to adapt this tool for use in a particular CSIRT, thus making its costs range from low to low-moderate.



Toronto Rehab
Everything Humanly Possible

Adapted SBAR Tool
(Abbreviated)

S

SITUATION

Your name and service

Briefly state the problem and when it started

B

BACKGROUND

Diagnosis and co-morbidities

Other relevant background clinical information

- ❑ Medications
- ❑ Specialists and procedures in place

A

ASSESSMENT

What do you think the problem is?

- ❑ Physical
- ❑ Cognitive
- ❑ Emotional
- ❑ Functional
- ❑ Support/Care System

What is your assessment of the situation?

R

RECOMMENDATION

What do you suggest needs to be done?

What are you requesting?

Is everyone clear about what needs to be done?

Figure F.2b. Sample abbreviated SBAR tool
Note: From "SBAR: A shared structure for effective team communication: 2nd Edition," by B. Trentham, A., Andreoli, N. Boaro, K. Velji and C. Fancott, 2010, p. 5. Copyright 2010 by Toronto Rehabilitation Institute. Reprinted with permission.

[6] This is a technical medical term meaning that all of a patient's medical history is compiled together accurately and in a single location so that healthcare professionals can be fully informed at all patient transition points ("Medication Reconciliation," 2015).

Implementation costs are also relatively low based on the time necessary for introduction, training, and follow-up on proper usage. The SBAR protocol only works if everyone uses it consistently, and proper training and monitoring are critical to ensure successful adoption of the handoff protocol. In addition, it is very easy for employees who are accustomed to one way of doing things to reject or rebuff initiatives to change the status quo. Therefore, it is critical to follow proper change management practices when instituting team wide usage of the SBAR protocol (see Change Management section in the General Discussion).

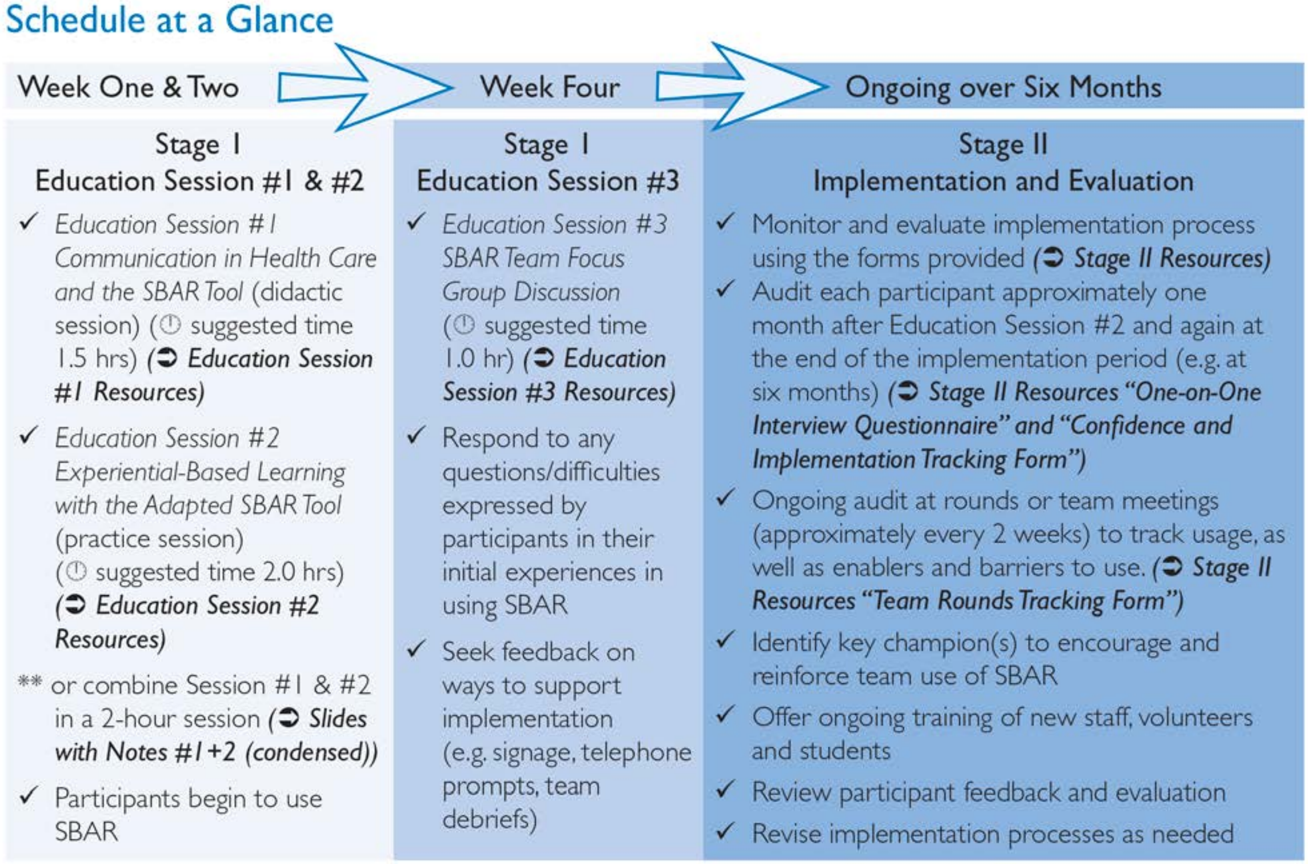
Figure F.3 gives a sample training and implementation timeline for the various information and feedback sessions that are suggested to be used. Generally speaking, several education sessions ranging from 1 to 2 hours each should be given over the course of a week or two, with a follow-up refresher and discussion group after a few weeks of use. Over the next several months, use of SBAR is monitored and evaluated, and teams discuss and provide feedback on the process as needed (Trentham, Andreoli, Boaro, Velji, & Fancott, 2010). Although time-intensive, this continuous monitoring and evaluation process ensures successful transition from development to implementation and maintenance phases.

Another common practice among EMS teams is to use **team wrap-up forms** in after-action reviews to evaluate their team processes. A typical team wrap-up form includes placeholders for the date and description of the event, a code indicating the category of the event (e.g., trauma, medical, stroke), a list of communication tools, and placeholders for lists of the things the team either did well or could improve (Turner, 2012). A meta-analysis of studies examining debriefs (Tannenbaum & Cerasoli, 2013) found an average of a 25% improvement in teamwork performance. That is a very significant improvement, especially when viewed in light of the relatively moderate cost of development and implementation of debrief/wrap-up forms. The compilation of team wrap-up forms in after-action reviews helps EMS teams to identify communication problems and address them during training and debriefing sessions. After-action reviews are discussed in more detail in the NPPO teams section below.

In addition to discussing cases after they are completed, research on EMS teams has found that short briefs before taking action, or momentary briefs during the action process, can also improve work outcomes. Tybinski and colleagues (2012) found that having this kind of **pre-briefing** "time-out" to go over the procedure and discuss the characteristics of the situation is important above and beyond just going through a checklist of required actions. One study on briefings found that team communication scores increased anywhere from 27% to 125% for various teams who used this strategy, and that overall patient

Figure F.3. Sample SBAR training timeline

Note: From "SBAR: A shared structure for effective team communication: 2nd Edition," by B. Trentham, A., Andreoli, N. Boaro, K. Velji and C. Fancott, 2010, p. 2. Copyright 2010 by Toronto Rehabilitation Institute. Reprinted with permission.



Schedule at a Glance

Week One & Two	Week Four	Ongoing over Six Months
Stage I Education Session #1 & #2	Stage I Education Session #3	Stage II Implementation and Evaluation
✓ *Education Session #1 Communication in Health Care and the SBAR Tool* (didactic session) (⏱ suggested time 1.5 hrs) ***(➲ Education Session #1 Resources)*** ✓ *Education Session #2 Experiential-Based Learning with the Adapted SBAR Tool* (practice session) (⏱ suggested time 2.0 hrs) ***(➲ Education Session #2 Resources)*** ** or combine Session #1 & #2 in a 2-hour session ***(➲ Slides with Notes #1+2 (condensed))*** ✓ Participants begin to use SBAR	✓ *Education Session #3 SBAR Team Focus Group Discussion* (⏱ suggested time 1.0 hr) ***(➲ Education Session #3 Resources)*** ✓ Respond to any questions/difficulties expressed by participants in their initial experiences in using SBAR ✓ Seek feedback on ways to support implementation (e.g. signage, telephone prompts, team debriefs)	✓ Monitor and evaluate implementation process using the forms provided ***(➲ Stage II Resources)*** ✓ Audit each participant approximately one month after Education Session #2 and again at the end of the implementation period (e.g. at six months) ***(➲ Stage II Resources "One-on-One Interview Questionnaire" and "Confidence and Implementation Tracking Form")*** ✓ Ongoing audit at rounds or team meetings (approximately every 2 weeks) to track usage, as well as enablers and barriers to use. ***(➲ Stage II Resources "Team Rounds Tracking Form")*** ✓ Identify key champion(s) to encourage and reinforce team use of SBAR ✓ Offer ongoing training of new staff, volunteers and students ✓ Review participant feedback and evaluation ✓ Revise implementation processes as needed

treatment quality improved by 8% to 11% (Awad et al., 2005).

In order to conduct the pre-brief, team members come together to momentarily go through key information pertaining to the situation at hand, what needs to be done, who is present, any anticipated problems, as well as whether proper documentation is available. They then discuss more details of the case (Awad et al., 2005).

Although seemingly simple, trainings for pre-briefs should first consist of general knowledge instruction on what steps are involved. Practice, role-playing exercises, and exposure to training films or vignettes should also be part of the training, so that employees can learn why this process is important. Finally, trainees should practice going through all the steps as a team and should learn how to identify any problems of poorly conducted pre-briefs in order to improve their standards for communication (Awad et al., 2005).

While development costs associated with pre-briefs are low due to the amount of extant material on pre-briefings and processes, implementation costs are low to moderate because not much time is required for proper training and instruction and because not much time is required by leaders and management to ensure that the strategy is being performed properly and consistently.

Trust strategies from EMS teams. Trust among EMS team members increases information sharing as well as willingness to seek information, accept feedback, and admit mistakes (Baker, Day, & Salas, 2006). For example, nurses are more willing to seek advice from other nurses and physicians whom they perceive as trustworthy, and, under conditions of uncertainty, seeking advice from another team member reduces medical errors (Hofmann, Lei, & Grant, 2009; Leach & Mayo, 2013). The importance of trust is greater during times of high stress, when speaking up and crucial communication become more important as predictors of patient safety and quality of care (Maxfield, Grenny, McMillan, Paterson, & Switzler, 2005).

Luckily, another protocol emphasized in EMS training has been developed specifically to address this issue. The **CUS** (meaning, "I am Concerned!, I am Uncomfortable!, This is a Safety issue!"; Capella et al., 2010, p. 440) protocol improves communication and speaking-up behavior during stressful times by eliminating sarcastic comments and increasing clarity among team members, and, as a result, improves feelings of mutual support (e.g., Capella et al., 2010). Specifically, the effective use of CUS requires all team members to be on alert for the key CUS phrases (viz., "I am Concerned!", "I am Uncomfortable!", "This is a Safety issue!"); when someone says one of those key phrases it should be understood that sarcasm and potentially confusing expressions are to be avoided. CUS is to be utilized in situations where an individual feels there is a major concern not being addressed or does not feel like the proper course of action is being taken. Thus, when it is used, not only do present team members immediately understand the level of concern being raised, but also whoever is leading the course of action becomes responsible for addressing that individual's concern (Maguire, Bremner, Bennett, & VanBrackle, 2015).

This relatively simple technique has been shown to have dramatic effects on teamwork processes. Capella et al. (2010) showed that CUS (along with a few other communication interventions) marked improvements across a number of teamwork areas: leadership (20% improvement), situation monitoring (18%), mutual support (16%), communication (53%), and overall teamwork (18%). It was also found that the average time (in minutes) to transition from one phase of patients' emergency care to another was reduced by 26% (Capella et al., 2010).

Similar to medical workers, CSIRT members often work in stressful situations and are required to effectively communicate with team members in such situations (West-Brown, Stickvoort, Kossakowski, Killcrece, & Ruefle, 2003). Thus, CSIRT members can benefit from using the CUS protocol to communicate their stress to others. Some example situations in which the CUS protocol might be useful include when an analyst feels overwhelmed (either through stress or fatigue) and needs to communicate to their team or leader that their ability to perform tasks is impaired, when an analyst believes that a critical element of an incident is not being addressed, or when an analyst comes across a situation or event that they are unfamiliar with but have an underlying feeling of concern about what is going on. They can use predetermined phrases such as "I am concerned!" and "I am uncomfortable!" to request a team member or leader to come over and review or discuss what was discovered.

Although the CUS protocol has already been designed, the development of this protocol requires training the team members for the proper use of CUS. Thus, there are low-moderate development costs that depend on who (i.e., internal vs. external specialists) delivers the training and the training method (e.g., lecture vs. simulation) chosen for the team members. In addition, implementation cost can be moderate, partially due to the requisite training, but also because of the relative time investment in order to successfully transition CUS into already established work norms (see the Change Management section in the General Discussion). The use of CUS would need to be constantly monitored and evaluated in order to understand whether or not it is being used properly and to assess the impact it has on work outcomes.

In addition to the CUS protocol, EMS teams encourage trust-building norms similar to those used by MR teams mentioned earlier. Medical team members who developed mutual trust were encouraged to admit their mistakes and, as a result, medical errors were reduced because team members learned from their failures and improved upon them (Edmondson, 2003; 2004). Edmondson (2003) also showed that improved mutual trust resulted in increased team learning.

EMS teams summary. The long history of EMS teams and the criticality of their effective functioning have garnered the attention of researchers for decades. Due to the similarity of teamwork requirements between EMS teams and CSIRTs, interventions found to be effective in the former should also be beneficial for the latter. Specifically, from EMS teams, CSIRTs can learn to improve their communication through checklists, handoff protocols, and wrap-up forms, and encourage trust through the development of norms like CUS. To help CSIRTs maximize their investment, a complete cost-effectiveness breakdown and discussion of when one recommendation should be favored is presented in the General Discussion section (see also Table F.1 and Table F.2).

F.3.3 NUCLEAR POWER PLANT OPERATING TEAMS

As the name might suggest, Nuclear Power Plant Operating (NPPO) teams work in nuclear power plants and control the functioning of the reactors (i.e., safely controlling how much power is produced). Such teams have the responsibility for controlling power plant systems and maintaining system equilibrium (Waller & Jehn, 2000; Waller, Gupta, & Giambatista, 2004). They do so by attending to system monitors, interpreting signals and data, and making decisions in response to possible events and incidents. As with CSIRTs, such decisions need to be made in time-urgent and high-stakes circumstances. If an abnormality is discovered, NPPO teams must quickly determine where the problem is coming from, decide on the appropriate action(s) to properly resolve the issue, and adequately record their action process in logbooks (*Occupational Outlook Handbook*. 2014).

While CSIRTs do not experience the same kind of physical danger as those working at a nuclear power plant, the underlying goals, and some of the related prevention behaviors, are similar. CSIRTs' main goals are to keep their networks clear of problems such as unauthorized users and to keep the networks as secure as possible so as to maintain the functionality of their constituencies' core business operations. Trying to control for human error and using forecasting techniques to evaluate how events can develop into possible threats, as well as knowing the possible consequences of outcomes, can aid CSIRTs in achieving these goals. Both the processes and the operating environments of NPPO teams closely mirror that of CSIRTs, and interventions to improve the functioning of NPPO teams should aid CSIRTs similarly.

Shared mental model recommendations from NPPO teams. As introduced when discussing MR teams, a shared understanding of how an operation works (i.e., a shared mental model) allows team members to more clearly recognize how their activities and functions are to be integrated in ways that improve the team's ability to successfully coordinate actions during complex tasks (Pearsall, Ellis, & Bell, 2010). A shared mental model also allows members to anticipate each other's needs and to know what behaviors must occur for effective task completion (Pearsall, et al., 2010). Shared knowledge is critical to effective performance in both NPPO teams and CSIRTs. Frye (1988) estimated that 50% of nuclear power's "significant events" were due to human errors. It was suggested that the errors were not due to the operators' inability to take appropriate action, but the control teams' inability to coordinate effectively--which is vital to successful performance of the NPPO teams (Lin, Hsieh, Tsai, Yang, & Yenn, 2011). A strategy that is suggested to improve coordination within NPPO teams is cross-training (e.g., Guerlain & Bullemer, 1996; "Nuclear power plant organization and staffing," 1998; "Recruitment, qualification and training," 2002).

Cross-training, which is "an instructional strategy in which each team member is trained in the duties of his or her teammates" (Volpe, Cannon-Bowers, Salas, & Spector, 1996, p. 87), increases shared mental models among team members by providing opportunities for individuals to obtain knowledge of their team members' roles (i.e., interpositional knowledge) (Cannon-Bowers, Salas, Blickensderfer, & Bowers, 1998; Ellis & Pearsall, 2011). Interpositional knowledge allows teams to more effectively understand each other's needs and responsibilities while coordinating actions (Cannon-Bowers et al., 1998; Salas, Nichols, & Driskell, 2007; Volpe et al., 1996). Studies comparing cross-trained individuals to those who were not cross-trained have demonstrated that cross-training increases shared mental model accuracy during high work demand situations by 24% (Ellis & Pearsall, 2011) and by 33% (Espevik, Johnsen, & Eid, 2011). Finally, teams already possessing strong team dynamics (e.g., shared mental models and transactive memory systems, or the shared understanding of who on the team has what knowledge) scored almost twice as high on performance measures after three training sessions as other teams going through the same training (Espevik et al., 2011).

Cost estimates of cross-training vary by its types: positional clarification, positional modeling, and positional rotation (Blickensderfer, Cannon-Bowers, & Salas, 1998). Positional clarification involves providing team members with information about the functions and role activities of others on the team (or activities of other teams) (Marks, Sabella, Burke, & Zaccaro, 2002). Development cost of positional clarification can be minimal as long as clear job descriptions are available for the team members, the CSIRT manager has a clear understanding of each team member's role, and/or each individual creates a short document describing his or her work tasks. Implementation cost can also be minimal as the team members can explicitly be told the tasks and responsibilities of other team members during onboarding or training exercises. This allows team members to have a better understanding of everyone's roles without requiring additional training time.

Positional modeling involves team members acquiring information about other team roles and functions by watching current role incumbents modeling work activities or by watching videos of functional activities (Marks et al., 2002). Shadowing other team members during the onboarding process and/or during a training exercise can provide analysts with the opportunity to observe another member's tasks and responsibilities, allowing another chance to understand how other teammates respond to certain work situations, via positional modeling. Positional modeling can cost a bit more than positional clarification depending on the training materials (e.g., videos) to be developed and the time spent by the trainees observing other team members.

Positional rotation, one of the most common forms of cross-training, entails having team members work for a limited time in team roles and positions different from their own (Marks, et al., 2002). These can be within the member's own team or on other teams. In real work contexts, this can be established by a team member either simulating another team member's role within a training session or rotating through the team and periodically taking new roles. Although the positional rotation approach makes the most significant impact on the transfer of skills and knowledge (e.g., Marks et al., 2002), one of the short-term pitfalls is that team members who are put into roles with which they are unfamiliar will initially have lower productivity and effectiveness. This means the benefits of the training will be established over a period of several weeks or months (Ebeling & Lee, 1994; Espevik et al., 2011).

Overall, cross-training can have a rather high implementation cost depending on which approach is taken, with positional clarification the least and positional rotation the most "expensive." Although cross-training can be conducted outside regular working hours, this may result in overtime pay, which will temporarily increase overhead costs (Ebeling & Lee, 1994). Another approach is to have cross-training occur during regular work hours, but to establish time limits on how much a particular employee can spend on the the skills and responsibilities needed for other jobs or functions (e.g., no fewer than 4 and no more than 16 hours per week, up to a maximum of 100 practice hours; *U.C. Davis Health System*, 2009). Overall, we recommend that more workers be trained in low-cost, short-duration versions of cross-training and that only a select few participate in the higher-cost, longer-duration cross-training (Ebeling & Lee, 1994). Fortunately, to offset these implementation costs, there is relatively little cost associated with the development of these strategies. Additionally, as mentioned previously, improvements from cross-training are quite significant. Although these strategies may be utilized already in some high performing CSIRTs, we recommend that all CSIRTs engage in some form of cross-training to achieve the optimal amount of benefits associated with the shared experiences.

Learning from mistakes through **after-action reviews,** or investigative reports, is another strategy NPPO teams use to improve shared mental models. When a serious event or problem occurs at a nuclear power plant, investigative teams of 3-12 people from various departments often work together, over a period of time ranging from several days to a couple of weeks, in order to conduct interviews, inspect the plant and equipment, and review logbooks and other documentation. The goal of these actions is to draw informed conclusions about why the undesirable event occurred, diagnose the situation and articulate possible remedial actions (Carroll, Hatakenaka, & Rudolph, 2006). Although this kind of time- and labor-intensive review process may only be feasible for high-severity and high-profile incidents (and under conditions of government regulation), most CSIRTs have some sort of general incident review process. However, this process varies widely across CSIRTs. Therefore, it is important to highlight the benefits (and best practices) for proper debriefing.

On one extreme, there are CSIRT managers who view after-action reviews as a waste of time. For example, one manager stated in an interview: "I've been through so many of those, we have to have an actual after-action review, and it's a waste of time. And I hate wasting time. You know? It's like I hate double doing something. That drives me absolutely batty when stuff like that happens."[7] In the middle of the spectrum, some CSIRT members view after-action reviews as a required step for a manager or more senior analyst when an incident is marked closed, but discussion and follow-up only occurs when problems exist in the report (e.g., missing information). Finally, on the other extreme, there are some CSIRTs that conduct after-action reviews in a manner similar to what is supported by empirical evidence--these CSIRTs "always try to have a lessons learned session," especially for large scale incidents, that includes "people who have worked on it. If we look at large scale incidents, we try to make it broader and get more people involved."[8]

NPPO, MR, and EMS teams have all developed a number of best practices that have been shown to maximize the positive impact of after-action reviews.[9] The primary purpose of after-actions reviews is to contextualize and make sense of experiences by highlighting key learning opportunities that can lead to improved performance in future work (Busby, 1999). It is important to note that after-action reviews have been shown to be beneficial when conducted for both successful and failed events, as both extremes provide examples of what can be done well or poorly, respectively (Ellis & Davidi, 2005). Along these lines, CSIRTs analyze successful and failed cyber attacks to identify the indicators of different incidents so as to improve detection and resolution in future attacks (Hutchins, Cloppert, & Amin, 2011). We recommend that the quality of teamwork is also emphasized during these reviews by conducting after-action reviews with all individuals who performed the actions being reviewed, as well as their supervisors and anyone who was affected by the event (or a team representative if the team is large), as these other perspectives help provide more situational awareness about how certain actions can impact others within the team or externally.

As mentioned earlier, after-action reviews are used not only by NPPO teams but also by MR and EMS teams. Based on the research on the three teams, after-action reviews can be conducted in four phases (Ahmed et al., 2013; Ellis & Davidi, 2005; see also Salas et al., 2008, for a more detailed process). The first phase is self-explanation, during which the actors (i.e., the persons who actually conducted the actions being reviewed) should explain in their own words what they did and why, as well as what they saw as being done well (and why) and what they saw as not being done well (and why). This can be done by phrasing feedback in terms of missed opportunities for the team rather than failed decisions of individuals. For example, if an analyst missed a key piece of information, the question could be raised, "What can we as a team do to capitalize on similar opportunities in the future?" (see Shute, 2008, for a thorough review of guidance for providing what is known as formative feedback). The second phase is to verify the information provided. Humans are naturally susceptible to biases when recalling information (Ariely & Zakay, 2001; March, Sproull, & Tamuz, 1991), and, as such, it is important to confirm key pieces of information as a team in after-action reviews. To accomplish this, the team leader can uniformly ask for all individuals to provide the

[7] This quotation is from one of our CSIRT team-lead interviews.

[8] This quotation is from one of our CSIRT focus group interviews.

[9] Though our discussion of after-action reviews focuses on NPPO teams due to the critical nature of learning from past events (especially failures) in nuclear power plants, the research reported here is from all three types of teams (i.e., MR, EMS, and NPPO).

data they used to make key decisions; this would prevent anyone from feeling singled out and would be relatively easy if information has been properly documented in checklists or an incident management system. This process can potentially be improved by increasing trust (discussed earlier in this appendix) and by conducting the after-action review as soon as possible after the event to be reviewed is finalized (e.g., Garvin, Edmondson, & Gino, 2008). In the third phase, feedback from the team leader or management should be provided on both the outcome and the process followed along the way. Here, again, the feedback should pertain to both ideal and suboptimal aspects of the process and focus on team-specific actions (as opposed to focusing on specific individuals). Finally, after-action reviews should have a fourth, future-oriented phase (Ahmed et al., 2013) during which participants in the review should try to determine what actions can be taken to improve performance in the future and how to best implement those actions.

Effective after-action reviews can be relatively time intensive (e.g., for training exercises, the debrief period is often about 30 minutes) depending on the situation and amount of discussion necessary (e.g., Daniels et al., 2010; Maguire et al., 2015; Wood, Zaientz, & Lickteig, 2006), and, therefore, costly to implement after each key learning opportunity. However, they are relatively inexpensive to develop, and they greatly improve team processes. While CSIRTs often do not have the time to spend weeks, or even days, reviewing a team failure, shorter debriefs after any major event—success or failure—can help promote a shared understanding of what was done well and what should be improved and done differently in the future (Ellis & Davidi, 2005). Even shorter (e.g., about 10-20 minute) after-action reviews have been shown to improve performance by 20 to 25% (Tannenbaum & Cerasoli, 2012), as well as increase a number of other team effectiveness outcomes: openness of communication increases by 11%, cohesion by 15%, efficacy by 22%, and, most importantly, overall performance by over 50% (Villado & Arthur, 2013). In addition, the effects of having debriefs as regular working norms have shown longevity. One study from the medical field found that both one year and two years after debriefing training began, several key performance metrics improved, including around a 10% decrease in work delays, a 5% decrease in handoff issues, and an almost 20% increase in overall work quality (as reflected in case scores) (Wolf et al., 2010).

NPPO team summary. The potential impact of poor NPPO team performance could be catastrophic and the same could be said for CSIRTs. Both teams operate under extreme stress and must be able to coordinate their actions with teammates effectively. Teamwork strategies found to be effective in NPPOs should also be beneficial for CSIRTs. Specifically, from NPPO teams CSIRTs can learn to improve shared mental models through cross-training and after-action reviews. To help CSIRTs maximize their investment, a complete cost-effectiveness breakdown and discussion of when one recommendation should be favored is presented next, in the General Discussion (see also Table F.1 and Table F.2).

F.4 General Discussion

CSIRTs are increasingly becoming a critical part of an organization's ability to maintain business continuity. As such, effective CSIRT performance is fundamental to organizational success in the modern world, and this is clearly evident from the executive order released on February 12th, 2013, from President Obama that stated the importance of improving America's critical cybersecurity infrastructure. Toward this end, we have provided a variety of recommendations based on the vast amount of research conducted on team and teamwork effectiveness in other fields (i.e., MR, EMS, and NPPO teams) that CSIRTs can utilize. In particular, we have focused on the key teamwork abilities and attributes of adaptation, shared mental models, communication, and trust.

For each recommendation, we have also assessed and discussed the relative cost and effectiveness (i.e., benefit) that are important to evaluate prior to implementation. It would be difficult (and inadvisable) to attempt all of these recommendations at once, not only due to the time and financial burden but also because attempting too much change in process or work requirements at once is likely to result in a significant amount of resistance from employees (please see Ford, Ford, & D'Amelio, 2008, for a more thorough discussion). For that reason, CSIRTs should prioritize and focus on what will make the most significant impact on the effectiveness of their specific team. This can be done by assessing current team performance and identifying what areas need the most improvement.

To aid managers and CSIRTs in determining what recommendations would be most useful for their unique situation, we have summarized all of the strategies in this appendix in Table F.1, where we categorized them under varying cost and effectiveness analysis criteria. Although there are certain recommendations that produce a high effect relative to their cost (more on these below), there are a few points that are often overlooked when evaluating the total cost associated with implementing these kinds of recommendations. The required investment in change management--the process of getting individuals onboard with new initiatives--and the evaluation of performance gains (as a result of specific interventions) are both necessary considerations. Without proper change management practices, even the best interventions can fall short of their potential (see Balogun & Hope Hailey, 2004, and Pettinger, 2004, for approaches to managing change initiatives) or have a negative impact on employee performance and attitudes (Graetz, 2000); and without thorough evaluation of performance changes after a training is conducted, there is no way to know if any improvement has actually been achieved (see Kirkpatrick & Kirkpatrick, 2007 for a guide to evaluating effectiveness). Keeping these factors in mind, we first highlight the overall strongest recommendations discussed in this appendix, based on their relative cost effectiveness, and then we recommend strategies based on specific needs that a CSIRT might have.

F.4.1 TOP RECOMMENDATIONS OVERALL

In this section, we highlight three of the top recommendations. While every recommendation provided above was presented due to its demonstrated ability to increase team performance in analogous teams, some of the strategies are better suited for some teams over others (again, Table F.1 is a useful tool for determining what is advisable for a CSIRT based on specific needs). The recommendations presented here are those that (a) have the lowest ratio of required cost to acquired effectiveness (i.e., are the most cost effective) and (b) are considered to be actionable. These top recommendations are SBAR, checklists, and cross-training. As a reminder, more detailed information about each of these was provided earlier in this appendix.

SBAR. The SBAR (Situation, Background, Assessment, and Recommendation) handoff protocol used in EMS teams not only has a significant impact on a wide range of performance outcomes but also helps promote clear and accurate communication among team members while simultaneously creating a more cohesive shared mental model about what pieces of information are important or necessary to share in verbal and written communication. Although time is required for proper customization, training, and feedback, having teams practice and use this tool in daily work can help develop a strong sense of teamwork and team efficacy (Pham et al., 2012; Cziraki et al., 2008; Pettker et al., 2009; Riesenberg et al., 2009; Velji et al., 2008).

Checklists. Using checklists can provide a significant improvement on various performance metrics and reducing errors within a team. The greatest addition to CSIRT checklists would be the inclusion of teamwork-related items that encourage good interpersonal and work-related behaviors. These items could include "Explicitly acknowledge effective collaboration among team members" for leader checklists and "Introduce yourself and give brief description of your background" for ad hoc team member checklists (Wolf et al., 2010). Spending the requisite time to develop these kinds of specialized checklists as a team would not only help improve team communication and shared mental models, but also feelings of trust within the team. As noted above, many checklists for complex procedures can require a lot of time to create and implement, but adding interpersonal items (e.g., displays of good teamwork behaviors) to existing checklists can be accomplished relatively easily (Leonard et al., 2004; Lingard et al., 2008; Taylor et al., 2007).

Cross-training. The various ways to implement cross-training make it a very flexible strategy to help team members develop the core team skills discussed in this appendix. As presented earlier, researchers have defined three forms of cross-training (Blickensderfer et al., 1998). First, teaching members about others' responsibilities through positional clarification helps improve the shared understanding of others' needs. Having members shadow others or teaching members the key abilities of others through positional modeling also helps develop shared mental models and communication skills. Finally, positional rotation, even for short periods of time, can help develop these attributes even more, as well as promote trust in team members' abilities to get work done and perform as required. In terms of cost effectiveness, due to the relatively low investment of time required for development, we would recommend the process of teaching members about others' responsibilities as being one of the most cost effective strategies for improving team performance.

F.4.2 TOP RECOMMENDATIONS FOR PARTICULAR NEEDS

In this section, we provide several assessment questions for each teamwork ability (adaptation, shared mental models, communication, trust) that allows you to assess which recommendation(s) might be most suitable for your team members given their current working abilities and context. For more details about each recommendation, including more information about its process and how it can be implemented, please refer to its given section earlier in this appendix.

Does your team suffer from poor adaptation? Recall that adaptation is defined as how a team changes its behavior, in response to varied situations, to accomplish its goal (Burke et al., 2006). Teams can have difficulty adapting for many reasons. As such, we have presented three techniques to help increase team adaptation, each with a slightly different focus. To determine if your team is having trouble adapting and which strategy might be more helpful, ask yourself the following questions:

1. *Does your team have difficulty generating effective solutions to novel incidents during irregular incident response processes?* If so, then **critical thinking** training may be the most useful strategy because it focuses on handling mental overload that can impair decision-making in novel or unknown situations.
2. *Does your team adapt well under normal circumstances, but have breakdowns when there are stressors present (e.g., limited time, increased severity)?* If so, then **stress exposure training** may be the most useful strategy because it provides the mental tools a team needs to maintain its ability to adapt and perform adequately when a situation becomes hectic or stressful.
3. *Does your team tend to operate in constantly varying situations where certain resources (e.g., information support, technical expertise) might not always be available?* If so, **perturbation training** may be the most useful strategy because it emphasizes coping and performing beyond routine patterns.

Does your team suffer from poor shared mental models? Shared mental models are the team members' shared understanding of each person's task requirements and functional activities (Cannon-Bowers et al., 1993; Peterson et al., 2000). In practice, this means that team members have a mutual understanding for how things are done in the team and which team member holds what unique task-relevant knowledge or expertise. To diagnose if your team has poor shared mental models, and pinpoint which strategy may be best to correct the problem, ask yourself the following questions:

1. *Is your team relatively inexperienced, and does it have difficulty approaching problems in the same way as a team of experts?* If so, then **guided team self-correction**

training may be the most useful strategy because it is designed to have more novice team members approach problems like experts would do while simultaneously increasing all team members' understanding of accurate and appropriate team processes.

2. *Does your team have a hard time determining who should do which task? Do some tasks go undone because of this? Or do some tasks get duplicated?* If you answered "yes" to the first and to either of the following two questions, then the **commander's intent model** might be the best strategy for your team because it helps all team members understand everyone's unique role within the team, informs how different situations dictate different actions for everyone in the team, as well as focuses on the overall objective (i.e., team's goal or purpose) in a given situation.
3. *Does your team ask (too often) about who has the knowledge to handle a particular event? Do team members have trouble explaining "who knows what" within your team?* If you answered "yes" to either of these questions, then **cross-training** might be the most useful strategy because it helps employees learn about other team members' roles and specialized skills by (a) being told what they do, (b) watching them perform their tasks first hand, or (c) performing other team members roles for a period of time.
4. *Do your team members fail to inform each other of lessons learned (especially when they are the only ones who have been involved in incident resolution)? Do your team members fail to view errors as a valuable learning opportunity?* If you answered "yes" to either of these questions, then you may want to consider instituting the use of **structured after-action reviews** and, potentially, **team-wrap-up forms**. These are both appropriate tools for helping teams promote or maintain an ongoing shared understanding of what was done well and what should be improved and done differently in the future.

Does your team suffer from poor communication? Communication is central to teams performing effectively and is critical for cohesive, adaptive teams to exist (e.g., Cohen, Mohrman, et al., 1998; Pollack, 1998). Without knowing the right information to give to others, as well as the most effective way to communicate that information, work processes can be severely hindered (e.g., Jentsch, Salas, Sellin-Wolters, & Bowers, 1995). To help decide if your team has poor communication, and which strategy may be most effective, ask yourself the following questions:

1. *Does your team consistently take too much time in the middle of incident resolution to talk about what they are seeing and doing?* If so, the use of **briefings** before taking action could help eliminate some of these problems by improving team cohesion and allowing the team to be focused on the actions that are required to achieve the team objectives prior to beginning incident resolution.
2. *Do your team members feel as though the information they provide is not understood by the other members in your team or members of other teams? Do your team members have to ask multiple clarification questions when receiving information from the members of your team or other teams?* If you answered "yes" to either of these questions, then the use of the **SBAR** protocol might help because it is a way to standardize the key pieces of information communicated between individuals or teams during handoffs, and ensures that complete yet concise information is shared among all those involved during critical transition points.
3. *Does your team suffer from other types of communication breakdowns, such as lack of important information being shared or poor interpersonal communication abilities?* If so, then the use of **checklists** that include interpersonal interaction items can help identify and address these issues. The impact of checklists can be enhanced by using checklists during pre-brief meetings.

Do your team members lack trust in each other? Trust determines whether or not team members believe they can rely on each other in risky or dangerous situations (Mayer et al., 1995), and is, therefore, important for sustainable team performance. To help understand if your team has issues with trust, ask yourself the following questions:

1. *Do your team members feel comfortable admitting mistakes to each other without worrying about being judged or evaluated? Do your team members bring up tough problems and issues with each other?* If you answered "no" to these questions, then your team members might be lacking trust in each other. To address this concern you should consider instituting some working norms that facilitate trust development, like **encouraging open discussion of mistakes, asking for others' opinions,** and **finding similarities amongst team members,** as well as incorporating more structured protocols like **CUS (i.e., "I am Concerned!, I am Uncomfortable!, This is a Safety issue!"**; Capella et al., 2010, p. 440). CUS establishes a professional and trusting environment when handling serious incidents, or incidents that may result in certain team members feeling uncomfortable or worried about a particular course of action that may lead to severe consequences.

F.4.3 CHANGE MANAGEMENT

Although many of the recommendations provided in this appendix can be incorporated into existing training methods or programs, several of them (e.g., checklists, briefings, SBAR) require changes to routine work procedures and, therefore, may lead to resistance or other negative emotional or behavioral consequences for employees (e.g., Rafferty & Griffin, 2006). To help prevent these unintended consequences, in this section we summarize some key recommendations from the change management literature on how to successfully implement and enforce changes to work procedures.

One key method for supporting change at work is the use of change leaders, or agents. These are individuals who have the potential to influence others and who are willing to support and monitor implementation of the new procedures (e.g., Hayes, 2012). The change agents must accept that successful adoption requires not only time (often several months to a year), but also a cycle of support that includes gathering feedback from the users of the new procedures and garnering alliances with administrators who are in control of necessary resources (Bosk, Dixon-Woods, Goeschel, & Provonost, 2009). This strategy has been used successfully in medical organizations for the implementation of checklists (e.g., Bosk et al., 2009; Hayes, 2012). Other studies have found that active leader involvement and support were the strongest predictors of successful checklist implementation (Conley, Singer, Edmondson, Berry, & Gawande, 2011). One key aspect to keep in mind is that it is not effective to use a "command and control" process in which these leaders simply give a new procedure or tool to employees and instruct them to "just do it"; the lack of explanation and support, as well as the enforcement of the power hierarchy, can exacerbate resistance to new procedures (Bosk et al., 2009).

Other research suggests limiting the size of initial usage or making the new work procedure voluntary at first and waiting for support and willingness to grow before requiring usage across the organization (Hayes, 2012). Another way this could be accomplished is through the use of pilot tests on "implementation teams"--comprising members from different disciplines and different hierarchical levels--by receiving feedback from them on the new work procedure and the rollout process and making adjustments in the procedure or rollout accordingly (Hayes, 2012; Pronovost et al., 2006). This method has been proven effective (i.e., making subsequent, larger-scale implementation easier) in an expansive rollout of surgical checklists in Canada's healthcare system (Hayes, 2012). In cybersecurity communities, implementation teams can consist of members with different CSIRT roles such as network system administrators, technical writers, programmers or developers.

The use of implementation teams also provides an easier way to collect pre- and post-implementation data on the outcome (e.g., information sharing within the CSIRT) to accurately monitor both the initial impact of the new work procedure as well as any moderate- to long-term effects. This suggestion follows the recommendations of several reviews on appropriate change management techniques (e.g., Tetrick, Wuick, & Gilmore, 2012; Kotter & Schlesinger, 2008; Pronovost et al., 2006), which posit that, in addition to choosing the appropriate behaviors to address and selecting evidence-based strategies (which we have provided in this appendix), measures to evaluate the effectiveness of the strategies must be developed (which also requires a baseline of performance to be taken) and adherence to the strategy must be ensured.

Another way to ensure successful adoption of, and adherence to, new work procedures is to use data to create a "burning platform" (Hayes, 2012, p. 59; Kotter, 1996; Langley et al., 2009) to support the effectiveness of the changes. As data are collected, internal publication of the findings allows others (who have not yet utilized the new procedure) to recognize the impact of the new procedure on work outcomes as well as provides opportunities for feedback and open discussion of where else the procedure might be beneficial or where it might have unintended consequences (Hayes, 2012).

F.5 Conclusion

As the importance of cybersecurity work continues to become more visible, the pressure on CSIRTs to perform at higher levels will also increase. Finding ways to improve team effectiveness is crucial, and this can be accomplished using strategies that have been shown to be effective through well-designed research studies in other fields. In this paper, we have summarized several of these research-based strategies from teams with performance requirements similar to those of CSIRTs. We have also provided cost-effectiveness analyses to help managers and leaders assess which strategy might be the most appropriate for their specific situation and team needs.

References

Adams, B. D., Waldherr, S., Sartori, J., & Thomson, M. (2007). *Swift trust in distributed ad hoc teams* (No. DRDC-CR-2007-139). Toronto, CA: Department of National Defence, Defence Research and Development Canada. Retrieved from: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA477148

Ahmed, M., Arora, S., Russ, S., Darzi, A., Vincent, C., & Sevdalis, N. (2013). Operation debrief: a SHARP improvement in performance feedback in the operating room. *Annals of Surgery, 258*, 958-963.

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). *Defining incident management processes for CSIRTs: A work in progress* (No. CMU/SEI-2004-TR-015). Carnegie-Mellon University, Pittsburgh, PA. Software Engineering Institute.

Alonso, A., Baker, D. P., Holtzman, A., Day, R., King, H., Toomey, L., & Salas, E. (2006). Reducing medical error in the military health system: how can team training help? *Human Resource Management Review, 16*, 396-415.

Ariely, D., & Zakay, D. (2001). A timely account of the role of duration in decision making. *Acta Psychologica, 108*, 187-207.

Awad, S. S., Fagan, S. P., Bellows, C., Albo, D., Green-Rashad, B., De La Garza, M., & Berger, D. H. (2005). Bridging the communication gap in the operating room with medical team training. *The American Journal of Surgery, 190*, 770-774.

Baker, D. P., Day, R., & Salas, E. (2006). Teamwork as an essential component of high-reliability organizations. *Health Services Research, 41*, 1576-1598.

Baker, D. P., Gustafson, S., Beaubien, J. M., Salas, E., & Barach, P. (2005). *Medical team training programs in health care*. Agency For Healthcare Research And Quality Rockville, MD.

Balogun, J. & Hope Hailey, V. (2004). *Exploring strategic change*, 2nd ed. London: Prentice Hall.

Bergs, J., Hellings, J., Cleemput, I., Zurel, Ö., De Troyer, V., Van Hiel, M., ... & Vandijck, D. (2014). Systematic review and meta-analysis of the effect of the World Health Organization surgical safety checklist on postoperative complications. *British Journal of Surgery, 101*, 150-158.

Blair, A.I., & Hanna, J.B. (2009). Trust and partnering with the joint team (No. AU/AFF/003/2009-04). Maxwell Air Force Base, AL: Air Command and Staff College Air University. Retrieved from: www.dtic.mil/dtic/tr/fulltext/u2/a539800.pdf

Blankenship, V., Hnat, S. M., Hess, T. G., & Brown, D. R. (1984). Reciprocal interaction and similarity of personality attributes. *Journal of Social and Personal Relationships, 1*, 415-432.

Blickensderfer, E., Cannon-Bowers, J.A., & Salas, E. (1998). Cross-training and team performance. In J.A. Cannon-Bowers & E. Salas (Eds.), *Making decisions under stress: Implications for individual and team training* (pp. 299-311). Washington, DC: American Psychological Association.

Bosk, C. L., Dixon-Woods, M., Goeschel, C. A., & Pronovost, P. J. (2009). Reality check for checklists. *The Lancet, 374*, 444-445.

Brady, M. J. (2011). *Battlefield lessons: The forward air surgical team (FAST) response*. Carlisle, PA: U.S. Army War College.

Burke, C. S., Stagl, K. C., Salas, E., Pierce, L., & Kendall, D. (2006). Understanding team adaptation: a conceptual analysis and model. *Journal of Applied Psychology, 91*, 1189-1207.

Busby, J. S. (1999). The effectiveness of collective retrospection as a mechanism of organizational learning. *The Journal of Applied Behavioral Science, 35*, 109 –129.

Campbell, D. J. (1988). Task complexity: A review and analysis. *Academy of Management Review, 13*, 40-52.

Cannon-Bowers, J. A., Salas, E., Blickensderfer, E., & Bowers, C. A. (1998). The impact of cross-training and workload on team functioning: A replication and extension of initial findings. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 40*, 92-101.

Cannon-Bowers, J. A., Salas, E., & Converse, S. A. (1993). Shared mental models in expert team decision making. In N. J. Castellan, Jr. (Ed.), *Individual and group decision making: Current issues* (pp. 221-246). Hillsdale, N J: Erlbaum.

Cannon-Bowers J. A., Tannenbaum S. I., Salas E., & Volpe C.E. (1995). Defining team competencies and establishing team training requirements. In Guzzo R, Salas E (Eds.), *Team effectiveness and decision making in organizations* (pp. 333–380). San Francisco, CA: Jossey-Bass

Capella, J., Smith, S., Philp, A., Putnam, T., Gilbert, C., Fry, W., ... & ReMine, S. (2010). Teamwork training improves the clinical care of trauma patients. *Journal of Surgical Education, 67*, 439-443.

Carroll, J. S., Hatakenaka, S., & Rudolph, J. W. (2006). Naturalistic decision making and organizational learning in nuclear power plants: Negotiating meaning between managers and problem investigation teams. *Organization Studies, 27*, 1037-1057.

Cecchine, G., Morgan, F. E., Wermuth, M. A., Jackson, T., & Schaefer, A. G. (2013). *The US military response to the 2010 Haiti earthquake: Considerations for army leaders*. Rand Corporation.

Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Gorab, A. K. (2014). *An Organizational Psychology Perspective to Examining Computer Security Incident Response Teams. IEEE Security & Privacy, 5*, 61-67.

Cohen, M. S., Freeman, J. T., & Thompson, B. B. (1998). Critical thinking skills in tactical decision making: a model and a training strategy. In J. A. Cannon-Bowers & E. Salas (Eds.), *Making decision under stress: Implications for individual and team training* (pp. 155–190). Washington, DC: American Psychological Association.

Cohen, S. G., Mohrman, S. A., & Mohrman Jr, A. M. (1998). We can't get there unless we know where we are going: Direction setting for knowledge work teams. *Research on Managing Groups and Teams, 2*, 1-31.

Conley, D. M., Singer, S. J., Edmondson, L., Berry, W. R., & Gawande, A. A. (2011). Effective surgical safety checklist implementation. *Journal of the American College of Surgeons, 212*, 873-879.

Costa, A. C. (2003). Work team trust and effectiveness. *Personnel*

Review, 32, 605-622.

Crichton, M. (2001). Training for decision making during emergencies. *Horizons of Psychology, 10*, 7-22.

Crichton, M. T. (2009). Improving team effectiveness using tactical decision games. *Safety Science, 47*, 330-336.

Crichton, M. T., Flin, R., & Rattray, W. A. (2000). Training decision makers–tactical decision games. *Journal of Contingencies and Crisis Management, 8*, 208-217.

Cziraki, K., Lucas, J., Rogers, T., Page, L., Zimmerman, R., Hauer, L. A., ... & Gregoroff, S. (2007). Communication and relationship skills for rapid response teams at Hamilton Health Sciences. *Healthcare Quarterly* (Toronto, Ont.), *11*, 66-71.

Dalenberg, S., Vogelaar, A. L., & Beersma, B. (2009). The effect of a team strategy discussion on military team performance. *Military Psychology, 21*, 31-46.

Daniels, K., Arafeh, J., Clark, A., Waller, S., Druzin, M., & Chueh, J. (2010). Prospective randomized trial of simulation versus didactic teaching for obstetrical emergencies. *Simulation in Healthcare, 5*, 40-45.

Debra, M., Weick, K. E., & Kramer, R. M. (1995). Swift trust and temporary groups. In R. M. Kramer & T. R. Tyler (Eds.) *Trust in organizations: Frontiers of theory and research* (pp. 166-195). Thousand Oaks, CA: Sage.

Deering, S., Rosen, M. A., Ludi, V., Munroe, M., Pocrnich, A., Laky, C., & Napolitano, P. G. (2011). On the front lines of patient safety: implementation and evaluation of team training in Iraq. *Joint Commission Journal on Quality and Patient Safety, 37*, 350-356.

Dickson, M. W., Smith, D. B., Grojean, M. W., & Ehrhart, M. (2001). An organizational climate regarding ethics: The outcome of leader values and the practices that reflect them. *The Leadership Quarterly, 12*, 197-217.

Dietz, A. S., Pronovost, P. J., Mendez-Tellez, P. A., Wyskiel, R., Marsteller, J. A., Thompson, D. A., & Rosen, M. A. (2014). A systematic review of teamwork in the intensive care unit: What do we know about teamwork, team tasks, and improvement strategies? *Journal of Critical Care, 29*, 908-914.

Dirks, K. T., & Ferrin, D. L. (2001). The role of trust in organizational settings. *Organization Science, 12*, 450-467.

Driskell, J. E., & Johnston, J. H. (1998). Stress exposure training. In J. A. Cannon-Bowers & E. Salas (Eds.), *Making decisions under stress: Implications for individual and team training* (pp. 191-217). Washington, DC: American Psychological Association.

Driskell, J. E., Johnston, J. H., & Salas, E. (2001). Does stress training generalize to novel settings? *Human Factors: The Journal of the Human Factors and Ergonomics Society, 43*, 99-110.

Driskell, J. E., Salas, E., & Johnston, J. (1999). Does stress lead to a loss of team perspective? *Group dynamics: Theory, Research, and Practice, 3*, 291-302.

Dweck, C.S. (2003) Ability conceptions, motivation and development. *British Journal of Educational Psychology: Monograph Series, 2*,13-28.

Ebeling, A. C., & Lee, C. Y. (1994). Cross-training effectiveness and profitability. *The International Journal of Production Research, 32*, 2843-2859.

Edmondson, A. C. (2003). Speaking up in the operating room: How team leaders promote learning in interdisciplinary action teams. *Journal of Management Studies, 40*, 1419-1452.

Edmondson, A. C. (2004). Learning from failure in health care: frequent opportunities, pervasive barriers. *Quality and safety in Health Care, 13*, ii3-ii9.

Ellis, S., & Davidi, I. (2005). After-event reviews: drawing lessons from successful and failed experience. *Journal of Applied Psychology, 90*, 857-871.

Ellis, A. P., & Pearsall, M. J. (2011). Reducing the negative effects of stress in teams through cross-training: A job demands-resources model. *Group Dynamics: Theory, Research, and Practice, 15*, 16-31.

Espevik, R., Johnsen, B. H., & Eid, J. (2011). Outcomes of shared mental models of team members in cross training and high-intensity simulations. *Journal of Cognitive Engineering and Decision Making, 5*, 352-377.

Fernandez, R., Kozlowski, S. W., Shapiro, M. J., & Salas, E. (2008). Toward a definition of teamwork in emergency medicine. *Academic Emergency Medicine, 15*, 1104-1112.

Ford, J. D., Ford, L. W., & D'Amelio, A. (2008). Resistance to change: The rest of the story. *Academy of Management Review, 33*, 362-377.

Fourcade, A., Blache, J. L., Grenier, C., Bourgain, J. L., & Minvielle, E. (2011). Barriers to staff adoption of a surgical safety checklist. *BMJ Quality & Safety, 21*, 1-7.

Frye, S. R. (1988). *An approach to enhanced control room crew performance*. In IEEE 4th Conference on Human Factors and Power Plants (pp. 574-576). Monterey, CA: IEEE.

Garvin, D. A., Edmondson, A. C., & Gino, F. (2008). Is yours a learning organization? *Harvard Business Review, 86*, 109-116.

Gawande, A. (2009). *The checklist manifesto*. New York, NY: Metropolitan Books.

Gladstein, D. L., & Reilly, N. P. (1985). Group decision making under threat: The tycoon game. *Academy of Management Journal, 28*, 613-627.

Gonsalves, J. D. (1997). The tactical decision game: An invaluable training tool for developing junior leaders. *Armor Magazine*, 35-38. Retrieved from: http://www.ciar.org/ttk/mbt/armor/armor-magazine/armor-mag.1997.mj/3tdg97.pdf

Gorman, J. C., Cooke, N. J., & Amazeen, P. G. (2010). Training adaptive teams. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 52*, 1-13.

Graetz, F. (2000). Strategic change leadership, *Management Decision, 38*, 550–562.

Guerlain, S., & Bullemer, P. (1996), *User-initiated notification: A concept for aiding the monitoring activities of process control operators*. In Proceedings of the Human Factors and Ergonomics Society 40th Annual Meeting (pp. 283-287). Santa Monica, CA: HFES.

Haig, K. M., Sutton, S., & Whittington, J. (2006). SBAR: a shared mental model for improving communication between clinicians. *Joint Commission Journal on Quality and Patient Safety, 32*, 167-175.

Hall, T. J., Rudolph, J. W., & Cao, C. G. (2006). *Fixation and attention allocation in anesthesiology crisis management: An abstraction hierarchy perspective*. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (pp. 1064-1067). SAGE Publications.

Harden, C. S. W. (2013). Six things every plastic surgeon needs to know about teamwork training and checklists. *Aesthetic Surgery Journal, 33*, 443-448.

Hayes, C. (2012). Surgical safety checklist: improved patient safety through effective teamwork. *Healthcare Quarterly, 15*, 57-62.

Hedlund, E., Börjesson, M., & Österberg, J. (2015). *Team Learning in a Multinational Military Staff Exercise. Small Group Research*. doi: 1046496414568462.

Hefford, M., & Blick, G. (2012, 18 June). *Cost benefit analysis of the surgical safety checklist*. Retrieved from: http://www.srgexpert.com/wp-content/uploads/2015/08/Surgical-safety-checklist-CBA-report-18-June-2012.pdf

Hewlett-Packard. (2014, August). *Growing the security analyst: Hiring, training, and retention*. Retrieved from: http://www8.hcom/h20195/v2/getpdf.aspx/4AA5-3982ENN.pdf?ver=1.0

Hofmann, D. A., Lei, Z., & Grant, A. M. (2009). Seeking help in the shadow of doubt: the sensemaking processes underlying how nurses decide whom to ask for advice. *Journal of Applied Psychology, 94*, 1261-1274.

Holton, J. A. (2001). Building trust and collaboration in a virtual team. *Team Performance Management: An International Journal, 7*, 36-47.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. In L. Armistead (Ed.), Proceedings of the 6th International Conference on Informational Warfare and Security, (pp. 113-125). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.301.2845&rep=rep1&type=pdf#page=123

International Atomic Energy Agency. (1998). *Nuclear power plant organization and staffing for improved performance: Lessons learned*. Retrieved from: http://www-pub.iaea.org/MTCD/publications/PDF/te_1052_prn.pdf

International Atomic Energy Agency. (2002). *Recruitment, qualification, and training of personnel for nuclear power plants*. Retrieved from: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1140_scr.pdf

Jentsch, F. G., Salas, E., Sellin-Wolters, S., & Bowers, C. A. (1995, October). *Crew coordination behaviors as predictors of problem detection and decision making times*. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 20, 1350-1353. SAGE Publications.

Keinan, G. (1988) Decision making under stress: Scanning of alternatives under controllable and uncontrollable threats. *Journal of Personality and Social Psychology, 52*, 639-644.

Kiffin-Petersen, S. (2004). Trust: A neglected variable in team effectiveness research. *Journal of Management and Organization, 10*, 38-53.

King, H. B., Battles, J., Baker, D. P., Alonso, A., Salas, E., Webster, J., ... & Salisbury, M. (2008). TeamSTEPPS™: *Team Strategies and Tools to Enhance Performance and Patient Safety*. In: Henriksen K, Battles JB, Keyes MA, et al., editors. *Advances in Patient Safety: New Directions and Alternative Approaches* (Vol. 3: Performance and Tools). Rockville (MD): Agency for Healthcare Research and Quality (US); 2008 Aug. Retreived from: http://www.ncbi.nlm.nih.gov/books/NBK43686/

Kirkpatrick, D.L. & Kirkpatrick, J.D. (2007). *Implementing the four levels: A practical guide for effective evaluation of training programs*. San Francisco: Berrett-Koehler Publisher.

Klein, G. A. (1993). *A script for the commander's intent statement*. Fairborn, OH: Klein.

Klein, K. J., Ziegert, J. C., Knight, A. P., & Xiao, Y. (2006). Dynamic delegation: Shared, hierarchical, and deindividualized leadership in extreme action teams. *Administrative Science Quarterly, 51*, 590-621.

Kliarsky, A. (2011). *Responding to zero day threats*. Retreived from: http://www.sans.org/reading-room/whitepapers/incident/responding-zero-day-threats-33709

Kohn, L. T., J. M. Corrigan, & M. S. Donaldson. (1999). *To err is human*. Washington, DC: National Academy Press.

Kotter, J. P., & Schlesinger, L. A. (2008). Choosing strategies for change. *Harvard Business Review, 86*, 130-139.

Langley, G. J., Moen, R., Nolan, K. M., Nolan, T. W., Norman, C. L., & Provost, L. P. (2009). *The improvement guide: a practical approach to enhancing organizational performance*. John Wiley & Sons.

LeBlanc, V. R. (2009). The effects of acute stress on performance: implications for health professions education. *Academic Medicine, 84*, S25-S33.

Leach, L. S., & Mayo, A. M. (2013). Rapid response teams: qualitative analysis of their effectiveness. *American Journal of Critical Care, 22*, 198-210.

Lee, S. M., Ha, J. S., & Seong, P. H. (2011). CREAM-based communication error analysis method (CEAM) for nuclear power plant operators' communication. *Journal of Loss Prevention in the Process Industries, 24*, 90-97.

Leonard, M., Graham, S., & Bonacum, D. (2004). The human factor: the critical importance of effective teamwork and communication in providing safe care. *Quality and Safety in Health Care, 13*, i85-i90.

Lin, C. J., Hsieh, T. L., Tsai, P. J., Yang, C. W., & Yenn, T. C. (2011). Development of a team workload assessment technique for the main control room of advanced nuclear power plants. *Human Factors and Ergonomics in Manufacturing & Service Industries, 21*, 397-411.

Lingard, L., Regehr, G., Orser, B., Reznick, R., Baker, G. R., Doran, D., ... & Whyte, S. (2008). Evaluation of a preoperative checklist and team briefing among surgeons, nurses, and anesthesiologists to reduce failures in communication. *Archives of Surgery, 143*, 12-17.

Lloyd, A.S. (2001). *Military environmental response operation (MERO) support to the CINC's. Naval War College*, Newport, RI: Joint Military Operations Department.

Maguire, M. B. R., Bremner, M. N., Bennett, D. N., & VanBrackle, L. (2015). Evaluation of TeamSTEPPS integration across a curriculum regarding team attitudes: A longitudinal study. *Journal of Nursing Education and Practice, 5*, 131-138.

March, J. G., Sproull, L. S., & Tamuz, M. (1991). Learning from samples of one or fewer. *Organization Science, 2*, 1-13.

Marks, M. A., Sabella, M. J., Burke, C. S., & Zaccaro, S. J. (2002). The impact of cross-training on team effectiveness. *Journal of Applied Psychology, 87*, 3-13.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*, 709-734.

Maxfield, D., Grenny, J., McMillan, R., Patterson, K., & Switzler, A. (2005). *Silence kills: The seven crucial conversations for healthcare*. Retrieved from http://www.silencekills.com/PDL/SilenceKills.pdf

Medication reconciliation to prevent adverse drug events. (n.d.). Retrieved from http://www.ihi.org/topics/adesmedicationreconciliation/Pages/default.aspx

Mishra, A. (1996). *Organizational responses to crisis: The centrality of trust*. In R. M. Kramer, & T. R. Tyler (Eds.), Trust in organizations (pp. 261–287). Thousand Oaks, CA: Sage Publications, Inc.

Morey, J. C., Simon, R., Jay, G. D., & Rice, M. M. (2003). *A transition from aviation crew resource management to hospital emergency departments: The MedTeams story*. In R. S. Jensen (Ed.), Proceedings of the 12th International Symposium on Aviation Psychology (pp. 1–7). Dayton, OH: Wright State University Press.

Morrison, J. E., Moses, F. L., Fletcher, J. D., Roberts, E. J., & Quinkert, K. A. (2007). *A cost-benefit analysis applied to example proposals for army training and education research*. (No. IDA D-3469). Institute for Defense Analyses, Alexandria, VA.

Murphy, L. R. (2003). *Stress management at work: Secondary prevention of stress*. In M. J. Schabracq, J. A. M. Winnubst & C. L. Cooper (Eds.), Handbook of work and health psychology (pp. 533-548). Winchester, U.K.: John Wiley & Sons, Ltd.

Novak, D. W., & Lerner, M. J. (1968). Rejection as a consequence of perceived similarity. *Journal of Personality and Social Psychology, 9*, 147-152.

Occupational Outlook Handbook. (2014, January 8). *Power plant operators, distributors, and dispatchers*. [Online]. Retrieved from http://www.bls.gov/ooh/production/power-plant-operators-distributors-and-dispatchers.htm

O'Connor, P., Campbell, J., Newon, J., Melton, J., Salas, E., & Wilson, K. A. (2008). Crew resource management training effectiveness: a meta-analysis and some critical needs. *The International Journal of Aviation Psychology, 18*, 353-368.

Olison, F. W. (2012). *Building and understanding trust relationships*. Army War College Carlisle Barracks, PA.

Patterson, E. S., Roth, E. M., Woods, D. D., Chow, R., & Gomes, J. O. (2004). Handoff strategies in settings with high consequences for failure: lessons for health care operations. *International Journal for Quality in Health Care, 16*, 125-132.

Peake, C. (2003). *Red teaming: The art of ethical hacking*. SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/auditing/red-teaming-art-ethical-hacking-1272

Pearsall, M. J., Ellis, A. P., & Bell, B. S. (2010). Building the infrastructure: The effects of role identification behaviors on team cognition development and performance. *Journal of Applied Psychology, 95*, 192-200.

Peterson, E., Mitchell, T., Thompson, L., & Burr, R. (2000). Collective efficacy and aspects of shared mental models as predictors of performance over time in work groups. *Group Process & Intergroup Relations, 3*, 296 –316.

Pettinger, R. (2004) *Contemporary Strategic Management*. Basingstoke: Palgrave MacMillan.

Pettker, C. M., Thung, S. F., Norwitz, E. R., Buhimschi, C. S., Raab, C. A., Copel, J. A., ... & Funai, E. F. (2009). Impact of a comprehensive patient safety strategy on obstetric adverse events. *American Journal of Obstetrics and Gynecology, 200*, 492-e1.

Pham, J. C., Aswani, M. S., Rosen, M., Lee, H., Huddle, M., Weeks, K., & Pronovost, P. J. (2012). Reducing medical errors and adverse events. *Annual Review of Medicine, 63*, 447-463.

Pollack, B. N. (1998). Hierarchical linear modeling and the "unit of analysis" problem: A solution for analyzing responses of intact group members. *Group Dynamics: Theory, Research, and Practice, 2*, 299-312.

Priest, H. A., Stagl, K. C., Klein, C., Salas, E., (2006). Virtual Teams: Creating context for distributed teamwork. In C. Bowers, E. Salas, F. Jentsch (Eds.). *Creating high-tech teams: Practical guidance on work performance and technology* (pp. 185-212). Washington, DC, US: American Psychological Association.

Pronovost, P. J., Berenholtz, S. M., Goeschel, C. A., Needham, D. M., Sexton, J. B., Thompson, D. A., ... & Hunt, E. (2006). Creating high reliability in health care organizations. *Health Services Research, 41*, 1599-1617.

Rafferty, A. E., & Griffin, M. A. (2006). Perceptions of organizational change: a stress and coping perspective. *Journal of Applied Psychology, 91*, 1154-1162.

Ramthun, A. J., & Matkin, G. S. (2014). Leading dangerously: A case study of military teams and shared leadership in dangerous environments. *Journal of Leadership & Organizational Studies, 21*, 244-256.

Riesenberg, L. A., Leitzsch, J., & Little, B. W. (2009). Systematic review of handoff mnemonics literature. *American Journal of Medical Quality, 24*, 196-204.

Ross, J.M., Szalma, J.L., & Hancock, P.A. (2004). *Efficacy of transfer in simulation-based training: Implications for stress exposure training*. Proceedings of the Second Swedish-American Workshop on Modeling and Simulation, USA, 145-150.

Ryan, A. M., & Tippins, N. T. (2004). Attracting and selecting: What psychological research tells us. *Human Resource Management, 43*, 305-318.

Salas, E., DiazGranados, D., Klein, C., Burke, C. S., Stagl, K. C., Goodwin, G. F., & Halpin, S. M. (2008). Does team training improve team performance? A meta-analysis. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 50*, 903-933.

Salas, E., Nichols, D. R., & Driskell, J. E. (2007). Testing three team training strategies in intact teams a meta-analysis. *Small Group Research, 38*, 471-488.

Scarfone, K., Grance, T., & Masone, K. (2008, March). *Computer security incident handling guide* (Special Publication No. 800-16). Gaithersburg, MD: National Institute of Standards and Technology.

Schottke, D. (2010). *Emergency medical responder: Your first response in emergency care*. Jones & Bartlett Learning.

Schroder, H. M., Driver, M. J., & Streufert, S. (1967). *Human information processing*. Holt, Rinehart and Winston, New York.

Shadrick, S. B., Crabb, B. T., Lussier, J. W., & Burke, T. J. (2007). *Positive transfer of adaptive battlefield thinking skills*. (ARI Research Report 1873). Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.

Shadrick, S. B., & Fite, J. E. (2009). *Assessment of the captains in command training program for adaptive thinking skills* (Tech. Rep. 1240). Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.

Shadrick, S., & Lussier, J. (2004). *Assessment of the think like a commander training program* (Research Report No. 1824). Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.

Shute, V. J. (2008). Focus on formative feedback. *Review of Educational Research, 78*, 153-189.

Singer, R. N., Cauraugh, J. H., Murphy, M., Chen, D., & Lidor, R. (1991). Attentional control, distractors, and motor performance. *Human Performance, 4*, 55-69.

Smith-Jentsch, K. A., Cannon-Bowers, J. A., Tannenbaum, S. I., & Salas, E. (2008). Guided team self-correction impacts on team mental models, processes, and effectiveness. *Small Group Research, 39*, 303-327.

Spiker, V., Silverman, D. & Tourville, S. (1998). *Tactical team resource management effects on combat mission training performance*. Brooks Air Force Base, TX: U.S. Air Force Systems/Material Command.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., ... & Tetrick, L. E. (2015). *Improving cybersecurity incident response team effectiveness using teams-based research. Security & Privacy, IEEE, 13*, 20-29.

Sundstrom, E., De Meuse, K. P., & Futrell, D. (1990). Work teams: Applications and effectiveness. American Psychologist, 45, 120-133.

Sutcliffe, K. M., Lewton, E., & Rosenthal, M. M. (2004). Communication failures: an insidious contributor to medical mishaps. *Academic Medicine, 79*, 186-194.

Tannenbaum, S. I., & Cerasoli, C. P. (2013). Do team and individual debriefs enhance performance? A meta-analysis. Human Factors: *The Journal of the Human Factors and Ergonomics Society, 55*, 231-245.

Taylor, C. R., Hepworth, J. T., Buerhaus, P. I., Dittus, R., & Speroff, T. (2007). Effect of crew resource management on diabetes care and patient outcomes in an inner-city primary care clinic. *Quality and Safety in Health Care, 16*, 244-247.

Tetrick, L.E., Wuick, G.C., & Gilmore, P.L. (2012). Research in organizational interventions to improve well-being: Prevention and measurement perspectives. In C. Biron, M. Karanika-Murry, and C.L. Cooper (Eds.), *Managing psychosocial risks in the workplace: The role of process issues*. Routledge, Taylor & Francis Group, UK

Trentham, B., Andreoli, A., Boaro, N., Velji, K. & Fancott, C. (2010). *SBAR: A shared structure for effective team communication. An implementation toolkit*. 2nd Edition. Toronto Rehabilitation Institute: Toronto.

Tucker, J. S., & Gunther, K. M. (2009). The application of a model of adaptive performance to army leader behaviors. *Military Psychology, 21*, 315-333.

Turner, P. (2012). Implementation of TeamSTEPPS in the emergency department. Critical Care Nursing Quarterly, 35, 208-212.

Tybinski, M., Lyovkin, P., Sniegirova, V., & Kopec, D. (2012). Medical errors and their prevention. Health, 4, 165-172.

U.C. Davis Health System: *Program for employee cross-training*. (n.d.). [Online]. Retrieved from https://www.ucdmc.ucdavis.edu/hr/training/Forms/crosstrain.pdf

U.S. Army. (2014, September 30). *Squad overmatch study: Training human dimension to enhance performance*. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA613853

U.S. Army Sergeants Major Academy. (1993). Briefing guide. Retrieved from: http://www.au.af.mil/au/awc/awcgate/army/w122.htm

US Army Soldier and Biological Chemical Command (SBCCOM), & United States of America. (2003). *Chemical weapons improved response program (CWIRP) Playbook: Guidelines for responding to and managing a chemical weapons of mass destruction terrorist event*. Retrieved from: http://www.fta.dot.gov/documents/cwirp_playbook.pdf

U.S. Army Training and Doctrine Command (2009). *The army capstone concept operational adaptability: Operating under conditions of uncertainty and complexity in an era of persistent conflict, 2016-2028*. Fort Monroe, VA. Retrieved from: http://usacac.army.mil/CAC2/repository/capstone.pdf

U.S. Department of Health and Human Services (USDHHS) (2005). *Quality through collaboration: The future of rural & frontier emergency medical services in the U.S. health system*. Retrieved from: https://www.nasemso.org/Projects/RuralEMS/documents/QualityThroughCollaboration.pdf

Van Den Bosch, K., Helsdingen, A. S., & De Beer, M. M. (2004). *Training critical thinking for tactical command*. TNO Human Factors, Soesterberg, NL.

Van Dijk, R., & Van Dick, R. (2009). Navigating organizational change: change leaders, employee resistance and work-based identities. Journal of Change Management, 9, 143-163.

Velji, K., Baker, G. R., Fancott, C., Andreoli, A., Boaro, N., Tardif, G., ... & Sinclair, L. (2007). Effectiveness of an adapted SBAR communication tool for a rehabilitation setting. *Healthcare Quarterly (Toronto, Ont.), 11*, 72-79.

Verdaasdonk, E. G. G., Stassen, L. P. S., Widhiasmara, P. P., & Dankelman, J. (2009). Requirements for the design and implementation of checklists for surgical processes. *Surgical Endoscopy, 23*, 715-726.

Villado, A. J., & Arthur Jr., W. (2013). The comparative effect of subjective and objective after-action reviews on team performance on a complex task. *Journal of Applied Psychology, 98*, 514-528.

Volpe, C. E., Cannon-Bowers, J. A., Salas, E., & Spector, P. E. (1996). The impact of cross-training on team functioning: An empirical investigation. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 38*, 87-100.

Weaver, S. J., Lyons, R., DiazGranados, D., Rosen, M. A., Salas, E., Oglesby, J., ... & King, H. B. (2010). The anatomy of health care team training and the state of practice: a critical review. *Academic Medicine, 85*, 1746-1760.

Weaver, S.J., Rosen, M. A., Shekelle P.G., Wachter, R.M., Pronovost P.J., editors. *Team-training in healthcare: brief update review. Making healthcare safer II: an updated critical analysis of the evidence for patient safety practices*. Comparative effectiveness review no. 211. Rockville, MD: Agency for Healthcare Research and Quality. 472–479.

Waller, M. J., Gupta, N., & Giambatista, R. C. (2004). Effects of adaptive behaviors and shared mental models on control crew performance. *Management Science, 50*, 1534-1544.

Waller, M. J., & Jehn, K. A. (2000). Multiple system interfaces and task-based conflict: Technological and human factors. *Technology, 3*, 115-131.

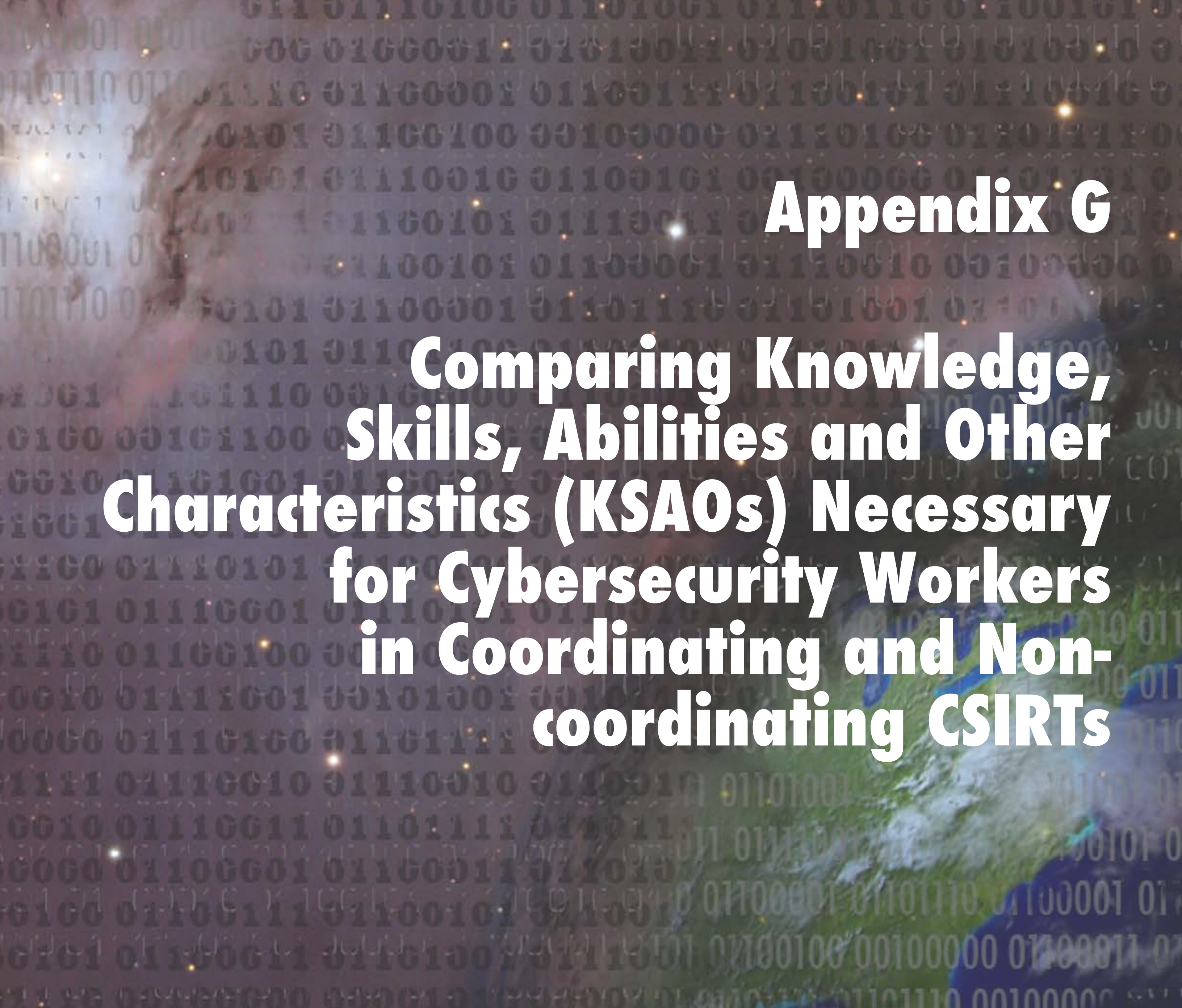
West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., & Ruefle, R. (2003). *Handbook for computer security incident response teams (CSIRTs)* (No. CMU/SEI-2003-HB-002). Carnegie-Mellon University, Pittsburgh, PA. Software Engineering Institute.

Whitman, M., Mattord, H., & Green, A. (2007). *Principles of incident response and disaster recovery*. Thomson Course Technology, Boston, MA

Wildman, J. L., Shuffler, M. L., Lazzara, E. H., Fiore, S. M., Burke, C. S., Salas, E., & Garven, S. (2012). Trust development in swift starting action teams: A multilevel framework. *Group & Organization Management, 37*, 138-170.

Wolf, F. A., Way, L. W., & Stewart, L. (2010). The efficacy of medical team training: improved team performance and decreased operating room delays: a detailed analysis of 4863 cases. *Annals of Surgery, 252*, 477-485.

Wood, S. D., Zaientz, J., & Lickteig, C. W. (2006). *Cooperative interface agents for networked command, control and communications: Phase II final report*. US Army Research Institute for the Behavioral and Social Sciences.



Appendix G

Comparing Knowledge, Skills, Abilities and Other Characteristics (KSAOs) Necessary for Cybersecurity Workers in Coordinating and Non-coordinating CSIRTs

Contents

G.1 Introduction

Cybersecurity incident response teams (CSIRTs) can vary along several dimensions. For example, they can differ based on the services they provide and their organization and structure (Cichonski, Millar, Grance, & Scarfone, 2013; Killcrece, Kossakowski, Ruefle, & Zajicek, 2003). One major organizational model that has drawn a lot of attention is the distinction between coordinating CSIRTs and non-coordinating CSIRTs. Coordinating CSIRTs often are broader in scope--providing services to help their constituent organizations address their cybersecurity needs--than non-coordinating CSIRTs. Coordinating CSIRTs' core services often are intrusion detection, advisory distribution, education and awareness, and information sharing, and coordinating CSIRTs often do not have authority over their constituent organizations. This is in contrast to non-coordinating CSIRTs who have onsite incident handling responsibilities and may or may not have authority over their constituencies. The purpose of this paper is to examine the knowledge, skills, abilities, and other characteristics (KSAOs) necessary for coordinating and non-coordinating CSIRTs and their members.

As part of a larger study, we conducted focus groups with several CSIRTs and their leaders. During these focus groups and interviews, CSIRT professionals were asked which KSAOs were necessary for effective performance. Based on a review of the literature on CSIRTs, it was anticipated that Communication, Trust, and Shared Knowledge of Unique Expertise, that is "who knows what" on the team, would be key topics in distinguishing coordinating CSIRTs from non-coordinating CSIRTs since coordination requires communication and information sharing, shared knowledge of unique expertise, and trust in order to distribute information. In the following section, we present findings from the focus groups and interviews relative to these three topics based on the type of CSIRT the participants represented.

G.2 Communication

According to our interviews and surveys with CSIRT members, the importance of communication processes and skills were confirmed as crucial for all CSIRT work. All performance functions at the team and MTS levels of our developed taxonomy (see Appendix A) included communication activities (for more discussion about the types and qualities of communications, the reader is referred to Chapter 5, "Communication Effectiveness in Incident Response." To summarize how focus group members and interviewees identified the importance of communication activities and to provide examples of the communication practices most often identified, we used a simplified framework of an incident response cycle (i.e., respond to incidents, triage, develop solutions, and conduct after-action reviews). Table G.1 presents the percentage of focus groups or interviews with cybersecurity professionals that indicated communication practices were important in each "phase" of incident response. Within this framework, the most commonly identified communication practices and behaviors for team effectiveness were in the incident response and triage phases. We found that other communication practices and behaviors within the developing incident solutions and conducting after-action reviews phases were commonly identified as important for MTS effectiveness.

To address our question as to whether communication was viewed as an important practice across all types of CSIRTs, we have plotted the percent of times communication was mentioned as important for CSIRT effectiveness in Figure G.1. All types of CSIRTs (i.e., coordinating, corporate, managed security service providers, and other) interviewed mentioned use of one or more communication practices as important to the incident response process. Although the percentages of participants mentioning each communication practice varied somewhat across the different types of CSIRTs, the pattern was consistent. Responding to incidents was mentioned most frequently, across the different types of CSIRTs followed by triage, then developing solutions, and conducting an after-action review.

These findings suggest that communication is an important ability and practice in all CSIRTs. It is less clear, given these data, whether communication is more important for coordinating CSIRTs than for non-coordinating CSIRTs. This may depend on which services are actually being provided by a CSIRT and the staffing patterns. For example, external communications may be assigned to one or two individuals within the CSIRT, rather than everyone being expected to be involved in external communications.

TABLE G.1 COMMUNICATION EXAMPLES BY INCIDENT RESPONSE PHASE (FROM TABLE 5.2, CHAPTER 5).

INCIDENT RESPONSE PHASE	COMMUNICATION PRACTICES IDENTIFIED BY FOCUS GROUP/INTERVIEW PARTICIPANTS	PERCENTAGE OF PARTICIPANTS WHO IDENTIFIED COMMUNICATION PRACTICES
Respond to incident	Discussion of how to share work; communication with affected constituency and stakeholders outside of constituency	88%
Triage	Discussion of how to assess and categorize identified incidents; information exchange to develop a shared understanding of the incident	65%
Develop solutions	Information exchange between teams to develop a shared understanding of incident; idea development between teams to select a course of action	60%
Conduct after-action review	Information exchange to evaluate procedures; revision of policies/ procedures if necessary; determine necessary after-action adaptation strategies	42%

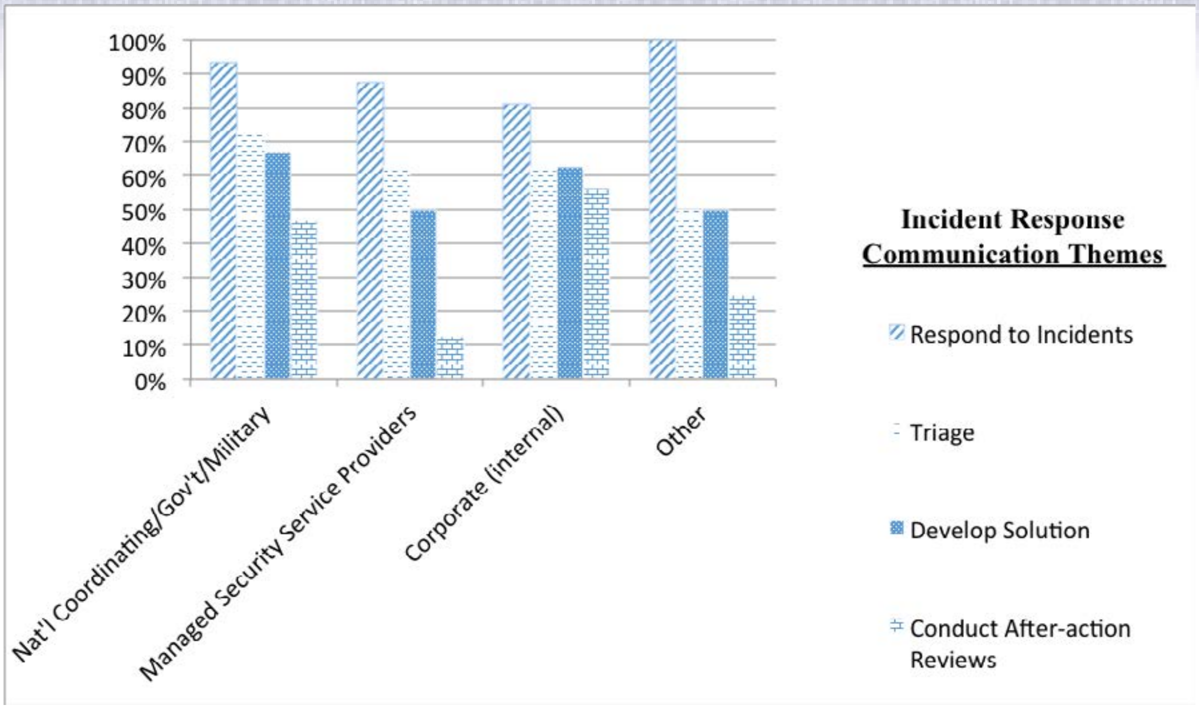


Figure G.1. Endorsement of Communication Themes by CSIRT Type. Note: Total Focus Groups (N=43); National Coordinating/Gov't/Military (N=15); Managed Security Service Providers (N=8); Corporate (N=16); Other (N=4).

G.2.1 SHARED KNOWLEDGE OF UNIQUE EXPERIENCE (SKUE)

In 80% (37 out of 46) of the focus groups we conducted, CSIRT members and managers indicated that knowing who had what expertise on the team was among the most important team and multi-team system (MTS) attributes for CSIRT effectiveness (see Chapter 8, "Shared Knowledge of Unique Expertise"). These focus group participants noted that such knowledge helped incident responders identify the nature of unusual events, triage them faster, and develop effective solutions. Our interviews indicated that successful teamwork (within and between teams) in response to an incident began with the identification of people who had the most appropriate expertise to work on that particular incident. Figure G.2 summarizes data from our focus groups indicating how often SKUE was mentioned as important in different types of CSIRTs and MTSs.

As is evident in Figure G.2, participants believed that SKUE was important for CSIRT effectiveness, regardless of in what type of CSIRT they were working.

G.2.2 TRUST

The third factor that we anticipated might distinguish between coordinating CSIRTs and non-coordinating CSIRTs was trust between members of CSIRTs to facilitate, as trust facilitates information sharing and collaboration (for more information on trust, see Chapter 9, "Trust in Teams and Incident Reponse Multiteam Systems"). Given that coordinating CSIRTs often do not have authority over their constituencies, it was considered that trust would be more important, whereas non-coordinating CSIRTs more frequently have some control over their constituents. Trust and psychological safety (i.e., feeling safe from embarrassment and ridicule for new ideas or mistakes) were mentioned as critical for CSIRT effectiveness in 72% (33 of 46) of our interviews with CSIRT members and leaders. These data indicate that CSIRT members consider trust to be an important factor for threat mitigation and incident resolution.

Most of the participants mentioned trust as important for CSIRT effectiveness, with the highest percentage of participants mentioning trust being from coordinating CSIRTs, followed closely by corporate CSIRT members (as shown in Figure 3). Surprisingly, very few of the employees in managed security service provider CSIRTs mentioned trust as important for CSIRT effectiveness. This finding may indicate that managed security service providers are contracted to provide a limited set of functions that do not include the same need for trusted relationships as other CSIRT types. Much more data would need to be collected to understand the reason for this differential finding and to see if this finding would generalize to other managed security service providers that were not included in this research. However, these findings do suggest that trust may be more important for coordinating CSIRTs than some other types of CSIRTs.

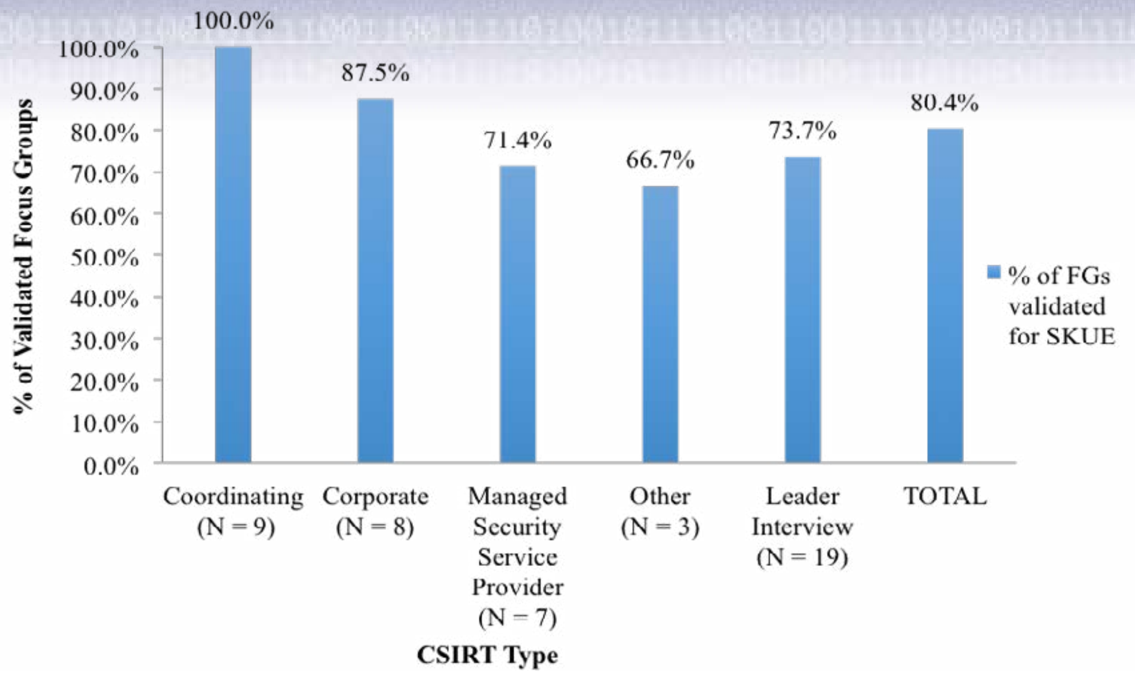


Figure G.2 Focus Group Support for Shared Knowledge of Unique Expertise (SKUE) (from Chapter 8 "Shared Knowledge of Unique Expertise")

G.3 Identifying Important KSAOs for Cybersecurity Incident Response Team Professionals

The above comparison was based on qualitative data from focus groups and interviews with CSIRT employees and leaders. This process gives some insight but has drawbacks in comparing coordinating CSIRTs with non-coordinating CSIRTs. To further hone our understanding of important KSAOs for CSIRT professionals, a multi-pronged approach was taken to first identify the KSAOs evident from multiple sources and then validate our conclusions from the perspective of cybersecurity professionals.

G.3.1 INITIAL IDENTIFICATION OF KSAOS

The first step was to create a preliminary list of KSAOs from all possible job functions within CSIRTs and MTSs. Specifically, a group of researchers derived KSAOs from five sources:

1. 12 job descriptions from the Occupational Information Network (O*NET; http://www.onetonline.org), which were identified using the keywords: "Security," "Cyber," "Network," "Computer," "Information," "Incident," "Response," and "Respond."
2. 111 job ads from major job search engines (e.g., Indeed.com), which were identified using the keywords: "CSIRT," "CERT," "SIRT," "Security," "Cyber," "Network," "Engineer," "Computer," "Information," "Incident," "Response," and "Respond."
3. The National Cybersecurity Workforce Framework (NICE, 2013).
4. 19 Popular, Industry, and Press Documents (PIPDs) on cybersecurity (e.g., Alberts, Dorofee, Killcrece, Ruefle, & Zajicek, 2004; Brechbühl, 2012) that specifically mentioned the KSAOs necessary for cybersecurity incident response.
5. Focus group transcripts obtained from interviews over a three-year period from two major time points: approximately the midpoint (December 2013) and towards the end (February 2015) of the data collection period.

The number of KSAOs by source, including duplicates between and within sources, are shown in Table 2.

G.3.2 REDUCTION OF KSAOS

Examination of the KSAOs from the different sources identified several redundancies across the various sources, indicating that

TABLE G.2 KSAOS FROM JOB SOURCES

SOURCE	ORIGINAL NUMBER OF KSAOS INCLUDING REDUNDANCIES ACROSS JOB SOURCES
O*NET	290
NICE	356
Job Ads	972
Literature	152
Focus Groups	409
Total	2,179

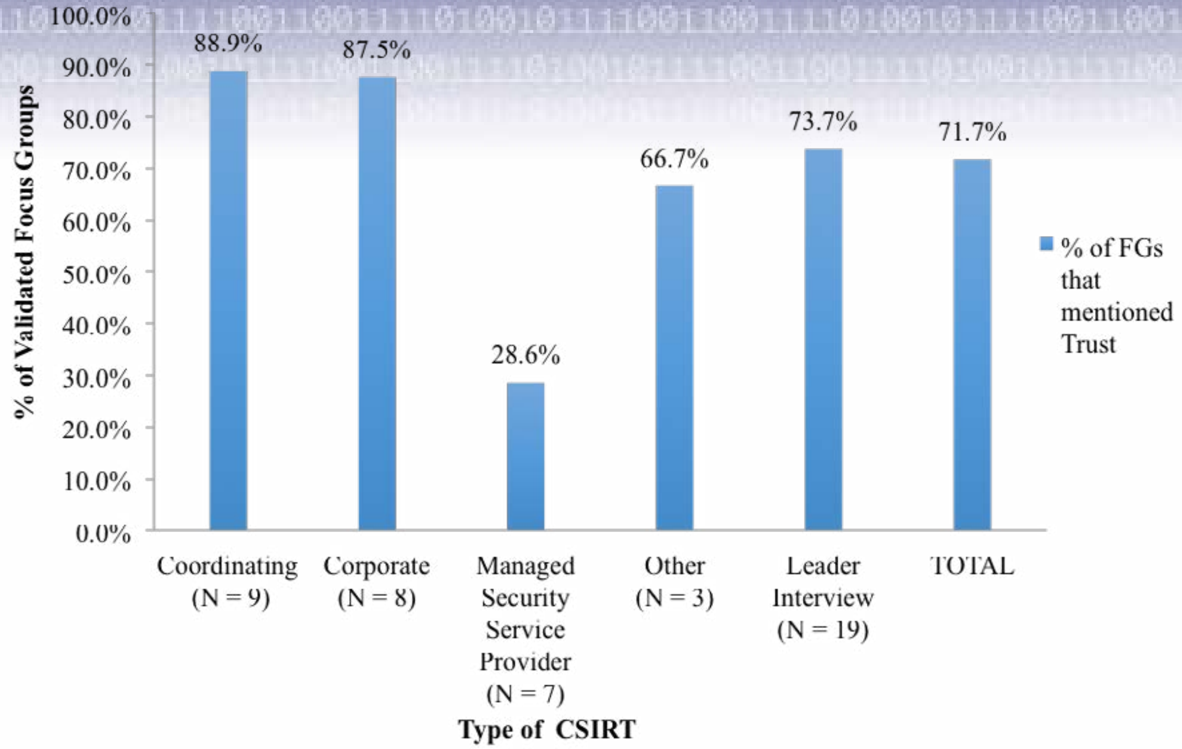


Figure G.3 Focus Group Support for Trust by CSIRT Type (from Chapter 9, "Trust in Teams and Incident Response Multiteam Systems")

the number of KSAOs identified could be reduced to a smaller, more manageable set of KSAOs without loss of information. It was also noted that the non-technical KSAOs fell into two categories: "social"—that is, involving interacting with others (e.g., communication skills) or "non-social"—that is, not involving interacting with others (e.g., cognitive ability). Therefore, the first step in the KSAO reduction process was to categorize each identified non-technical KSAO as either social or non-social. This was done by two research assistants who were subject matter experts in job analysis. Each KSAO then was screened to determine if it could be combined with another KSAO into a single unit because the two were essentially duplicates. Highly similar (but not identical) KSAOs (see next paragraph for an example) were identified and ultimately reworded into one comprehensive KSAO.

The National Cybersecurity Workforce Framework competencies (e.g., general IT knowledge, digital forensics, intrusion prevention) were used to initially group non-social KSAOs (e.g., "attention to details" and "thoroughness"). Non-technical KSAOs were categorized as "Social," "Cognitive," "Motivation," "Personality," and "Other," as suggested by project team subject matter experts.

G.3.3 EXPANSION OF SOURCES TO ORGANIZATIONAL SCIENCE LITERATURE

Non-technical KSAOs were not mentioned as frequently as technical KSAOs across all five of the sources initially accessed. This was counter to research in organizational psychology which has established that non-technical KSAOs are as important as technical KSAOs for performance, especially in team settings. Given this observation, social KSAOs, including team-level KSAOs, were identified from a review of peer-reviewed journal articles and scholarly books in the organizational psychology domain, using a process modeled after Pulakos, Arad, Donovan & Plamondon (2000) and Bateman, O'Neill, & Kenworthy-U'Ren (2002). The social KSAOs obtained through this literature review were then reduced to a taxonomy modeled after Stevens and Campion's procedure (1994) and adjusted to fit the National Cybersecurity Workforce Framework by the project team subject matter experts.

G.3.4 SUMMARY OF IDENTIFICATION OF RELEVANT KSAOs

There was a significant gap between what the focus group data showed and what was observed in existing sources (i.e., job ads, O*NET, and NICE). Four broad categories of KSAOs emerged: taskwork/physical, teamwork, cognitive factors, and personal character. The existing sources (i.e., job ads, O*NET, and NICE) overemphasized taskwork skills and did not provide sufficient differentiation with respect to attributes that foster effective teamwork.

G.3.5 KSAO SURVEY

Having identified relevant KSAOs, the next step in the process was to obtain input on the importance of the reduced set of KSAOs from cybersecurity professionals as further validation of important KSAOs for cybersecurity work. To do this, a survey was developed that included each of the KSAOs along with their definitions from various literatures. This survey was then distributed to cybersecurity personnel. These personnel were recruited in two organizations. One organization was a coordinating CSIRT, and the other one was a non-coordinating CSIRT. 56 people from the coordinating CSIRT,

TABLE G.3 DESCRIPTIVE ANALYSIS FOR ALL KSAOs

KSAO DESCRIPTION	CATEGORY	MEAN	SD	RWG
Willingness to fully engage in tasks and diligence to complete them	Character	4.82	0.42	0.83
Ability to acquire new knowledge through experiences	Cognitive	4.72	0.50	0.76
Extent to which a team member can be counted on to follow through on promises to complete tasks	Social/Team	4.70	0.49	0.68
Ability to work under stress resulting from time constraints, complex problems, unrealistic expectations, competing demands, and/or limited resources	Character	4.69	0.49	0.77
Skill of reviewing related information to develop and implement solutions to complex problems	Cognitive	4.68	0.56	0.70
Ability to explore unfamiliar topics in order to learn something new or seek out new challenges	Character	4.68	0.56	0.70
Skill of undertaking a task with minimal supervision	Character	4.66	0.52	0.74
Ability to perform higher mental processes of reasoning, remembering, understanding, and problem solving	Cognitive	4.65	0.57	0.69
Skill of strategically collecting and analyzing evidence surrounding cyber security issues	Cognitive	4.65	0.68	0.56
Skill of working with other members to solve problems and come to solutions that will help the team	Social/Team	4.61	0.54	0.73
Ability to make timely and difficult decisions about which course of action to take	Cognitive	4.60	0.54	0.62
Ability to achieve thoroughness and accuracy through concern for all the information involved	Character	4.59	0.62	0.63
Ability to put the goals of the team above his or her own	Social/Team	4.57	0.66	0.58
Ability to be proactive and take initiative	Character	4.57	0.56	0.70
Skill of readily adjusting oneself and responding effectively to a change in the situation	Character	4.57	0.56	0.70
Skill of understanding others and being understood by others; this skill can include speaking, writing, listening, etc.	Social/Team	4.56	0.58	0.67
Ability to persist in an action or purpose despite difficulties, obstacles, or discouragement	Character	4.52	0.61	0.65
Skill of helping other team members reach their full potential	Social/Team	4.52	0.66	0.58
Ability to explore novel, complex, or ambiguous solutions when confronted with a situation (e.g., solving a puzzle)	Character	4.52	0.66	0.89
Ability to maintain an objective attitude despite uncertain or unclear instructions, situations, or problems	Character	4.50	0.68	0.56
Skill of taking the view of another team member to understand an issue or problem from a different perspective	Social/Team	4.45	0.59	0.67
Skill of performing two or more tasks simultaneously	Character	4.44	0.74	0.63
Knowledge of ethical principles and values that are meaningful to the organization	Cognitive	4.38	0.76	0.44
Ability to be unconventional in thinking and bold in new ideas	Cognitive	4.36	0.73	0.49
Extent to which a team has a mutual understanding of the job, task and/or technology	Social/Team	4.34	0.74	0.47
Extent to which a team has a mutual understanding of how team members are supposed to act to get something done – shared team interaction models	Social/Team	4.32	0.75	0.46
Ability to generate novel and useful ideas, for the development of improved processes, processes, services, or products	Cognitive	4.27	0.71	0.52
Skill of planning the amount of time spent on specific activities, in order to increase effectiveness and/or efficiency	Cognitive	4.24	0.80	0.38
Skill of building effective working relationships beyond the team	Social/Team	4.23	0.74	0.62
Ability to modify one's behavior to meet the requirements of the situation	Social/Team	4.23	0.71	0.52

Note: N = 88; Participants are from Coordinating CSIRT (N = 56), Non-Coordinating CSIRT (N = 29), and Other (N = 3).
*** Rwg is an index of rater agreement on importance of the KSAO.
Specific references and sources for the KSAO definitions in this table are available from Lois Tetrick at ltetrick@gmu.edu.

TABLE G.3 DESCRIPTIVE ANALYSIS FOR ALL KSAOs (CONTINUED)

KSAO DESCRIPTION	CATEGORY	MEAN	SD	RWG
Tolerance adhering to rules and procedures despite personal opinion	Character	4.19	0.92	0.19
Ability to maintain an optimistic disposition	Character	4.17	0.84	0.49
Skill of constructively handling disagreements so that everyone involved comes to a workable solution	Social/Team	4.16	0.79	0.41
Skill of responding to a product, process, or behavior; this may involve highlighting positive areas and suggesting areas of improvement where needed	Social/Team	4.15	0.70	0.52
Skill of managing one's feelings and emotions	Social/Team	4.14	0.78	0.42
Extent to which a team knows what skills and abilities all the team members possess	Social/Team	4.11	0.81	0.37
Strong feelings of excitement and enthusiasm for completing everyday cyber security tasks	Character	4.07	0.87	0.28
Ability to understand the intentions of team members and to pick up on unspoken social cues	Social/Team	4.03	0.84	0.34
Skill of influencing other team members through direction setting and motivational tactics	Social/Team	4.01	0.85	0.30
Knowledge of several academic disciplines (e.g., history, psychology) and/or or professional specializations (e.g., IT, software development) for use in approaching a topic or problem	Cognitive	4.00	0.90	0.23
Willingness to work shifts or be on call during weekends or non-standard work hours	Character	3.94	1.11	-0.18
Extent to which a team member is not arrogant	Character	3.92	0.96	0.11
Skill of convincing others to feel, think, or do something	Social/Team	3.89	0.92	0.19
Ability to sit for extended periods of time	Physical	3.81	1.14	-0.26
Skill of negotiating	Social/Team	3.43	1.08	-0.12
Knowledge of arithmetic algebra, geometry, calculus, statistics, algorithms, and their applications to cyber security scenarios (e.g. developing incident detection software)	Cognitive	3.34	1.07	-0.09

Note: N = 88; Participants are from Coordinating CSIRT (N = 56), Non-Coordinating CSIRT (N = 29), and Other (N = 3).
***** Rwg is an index of rater agreement on importance of the KSAO.**
Specific references and sources for the KSAO definitions in this table are available from Lois Tetrick at ltetrick@gmu.edu.

responded and 29 from the non-coordinating CSIRT responded. Three additional responses from individuals who were not associated with either of these two organizations, and whose CSIRT could not be identified as either a coordinating or a non-coordinating CSIRT, were also collected. Each respondent was asked to indicate how important each KSAO was for effective performance based on a scale from 1 – not important to 5 – very important. The KSAOs are listed below, rank ordered from the highest average rating of importance to the lowest (Mean). Also shown is the variability among participants in their ratings of importance (SD) and to what extent participants rated the importance of the specific KSAO the same (Rwg). An Rwg of at least .06 indicates agreement, and an Rwg below .60 generally indicates lack of agreement among the individuals' importance ratings.

Forty of the 46 KSAOs included in the survey received mean ratings higher than 4.0 (on a 5-point scale), indicating that most of the KSAOs identified were considered to be important for effective CSIRT performance. 20 of the 46 actually received mean ratings of 4.5 or higher. This was not surprising, as we selected KSAOs that appeared to be more important across the various sources.

The CSIRT personnel who responded to the survey tended to agree on the importance of the most highly rated KSAOs. As the average rating of the KSAO became lower, there was more variability among the ratings of the CSIRT personnel. This suggests that there might be differences in importance of some KSAOs based on contextual factors such as whether an individual was part of a coordinating CSIRT or personal/position factors such as leadership responsibilities and type of team (e.g. Malware, Forensics and Communication). However, additional analyses revealed that there were no reliable differences in mean importance ratings or interrater agreement based on whether the respondent was a member of a coordinating or non-coordinating CSIRT, had leadership responsibilities or not, or was on a specific type of team.

G.3.6 COMPARISON OF IMPORTANCE RATINGS FOR THE 20 MOST IMPORTANT KSAOS BY CATEGORY

Ten of the 20 most important KSAOs were categorized as Character KSAOs (see Table G.3 above), 5 were categorized as Cognitive KSAOs, and 5 were categorized as Social/Team KSAOs. The mean importance for Character and Cognitive KSAOs was only slightly higher than the Social/Team KSAOs. As shown in Table 4, the interrater agreement for these three categories was quite high, and the mean importance ratings were also very high.

Again, we examined whether there were differences in importance ratings based on any background characteristics of the respondents. As shown in Table G.5, CSIRT personnel who had worked longer in IT, cybersecurity, or their organization in general

TABLE G.4 DESCRIPTIVE ANALYSIS OF THE THREE CATEGORIES OF TOP 20 KSAOS

CATEGORY	NUMBER	MEAN	RWG
Character	10	4.62	0.92
Cognitive	5	4.67	0.92
Social/Team	5	4.59	0.91

Rwg is an index of rater agreement on importance of the KSAO.

tended to rate the cognitive KSAOs as more important compared to people who had been in the field or in their organization for a shorter time period. There were no differences in ratings of importance for the Character and Social/Team KSAOs based on experience.

TABLE G.5 CORRELATIONS BETWEEN TOP 20 KSAS AND TENURE

	TENURE	TENURE	TENURE	TENURE
Category	IT	Cybersecurity	Organization	Position
Character	.15	.14	.17	.12
Cognitive	.25*	.25*	.24*	.10
Social/ Team	.13	.04	.08	.11

Note: * p < .05 (i.e., statistically significant). All numbers are Pearson product moment correlation coefficients (r).

G.3.7 COMPARISON OF IMPORTANCE RATINGS FOR THE 26 LEAST IMPORTANT KSAOS BY CATEGORY

There were 26 KSAOs that were rated as less important than the previous 20 KSAOs, although the mean importance rating of these 26 KSAOs still indicated that they were viewed as important. As shown in Table 6, there was less agreement among the CSIRT professionals as to the importance of these 26 KSAOs. Six of these KSAOs were Character KSAOs, 6 were Cognitive KSAOs, and 13 were Social/Team related KSAOs.

Mean importance ratings for Character and Cognitive KSAOs were only slightly lower than those of Social/Team KSAOs. The interrater agreement for the ratings was lowest for the Character KSAOs and highest for the Social/Team KSAOs. These findings suggest that there is considerable consensus among the CSIRT professionals that these KSAOs are important for CSIRT effectiveness, even though they may be somewhat less important than the 20 KSAOs that were rated slightly higher. Interestingly, tenure was not related to the ratings of importance for these 26 KSAOs, contrary to what was found for the 20 most important KSAOs.

TABLE G.6 MEANS AND INTERRATER AGREEMENT ON IMPORTANCE FOR THE THREE CATEGORIES OF KSAOS WITH THE LOWEST RATINGS OF IMPORTANCE

CATEGORY	NUMBER	MEAN	RWG
Character	6	4.10	0.60
Cognitive	6	4.10	0.74
Social/Team	13	4.13	0.89

Rwg is an index of rater agreement on importance of the KSAO.

G.4 Summary and Conclusions

KSAOs for CSIRT professionals were derived from multiple sources. These included job ads; the NICE framework; O*Net; the popular, industry, and press documents on cybersecurity; focus groups conducted with CSIRT professionals; and the organizational science literature. Generally, these sources converged, although important non-technical KSAOs were underrepresented in several of the sources; this was especially the case for social and team KSAOs.

- In staffing CSIRTs, managers need to consider non-technical knowledge, skills, abilities, and other characteristics, not just technical knowledge and abilities.

Based on responses from CSIRT professionals to the validation survey, support was found for the importance of the KSAOs that were identified and are shown in Table G.3 above. The agreement as to the importance of the KSAOs was quite high, especially for the KSAOs which were rated the highest in importance. There was less agreement on the importance of those KSAOs which were rated as somewhat less important, although there were still acceptable levels of agreement for most of the KSAOs. The difference in agreement did not seem to be the result of individuals' background variables, type of CSIRT (coordinating versus non-coordinating) they were employed in, or the type of team (e.g. Malware, Forensics and Communication). One caveat should be mentioned, however, that the distribution of participants across various characteristics such as type of team was limiting in interpreting the data.

There was some suggestion based on the qualitative data obtained from the focus groups and interviews, compared to the KSAO survey data, that there might be differences in KSAOs required for personnel working in coordinating and non-coordinating CSIRTs. In the focus groups, we asked people to identify important KSAOs, whereas in the survey, we provided specific KSAOs that had already been identified from multiple sources as important. This difference in methodology may account for the seeming differences across the two data sets. Also, the numbers of participants were considerably different for the focus groups and interviews compared to the surveys, although more CSIRTs were represented in the focus groups and interviews.

The data do indicate that the core KSAOs have been identified, and they do not appear to differ in importance for coordinating and non-coordinating CSIRTs. It may be that it is possible to staff CSIRTs based on functions and services to be provided and that certain roles may require a somewhat different set of KSAOs. Further research is needed to determine optimal staffing combinations.

- The core KSAOs identified as most important do not differ between coordinating and non-coordinating CSIRTs.

References

Alberts, C., Dorofee, A., Killcrece, G., Reufle, R., & Zajicek, M. (2004). *Defining incident management processes for CSIRTs: A work in progress*. (No. CMU/SEI-2004-TR-015). Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.

Bateman, T. S., O'Neill, H., & Kenworthy-U'Ren, A. (2002). A hierarchical taxonomy of top managers' goals. *Journal of Applied Psychology, 87*, 1134-1148.

Brechbuhl, H., Bruce, R., Dynes, S., & Johnson, M.E. (2010). Protecting critical information infrastructure: Developing cybersecurity policy. *Information Technology for Development, 16*(1), 83-91.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2013). Computer security incident handling guide. *International Journal of Computer Research,20*(4), 459-530. Retrieved from http://search.proquest.com.mutex.gmu.edu/docview/1623314374?accountid=14541

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2013). Computer security incident handling guide. *International Journal of Computer Research,20*(4), 459-530. Retrieved from http://search.proquest.com.mutex.gmu.edu/docview/1623314374?accountid=14541

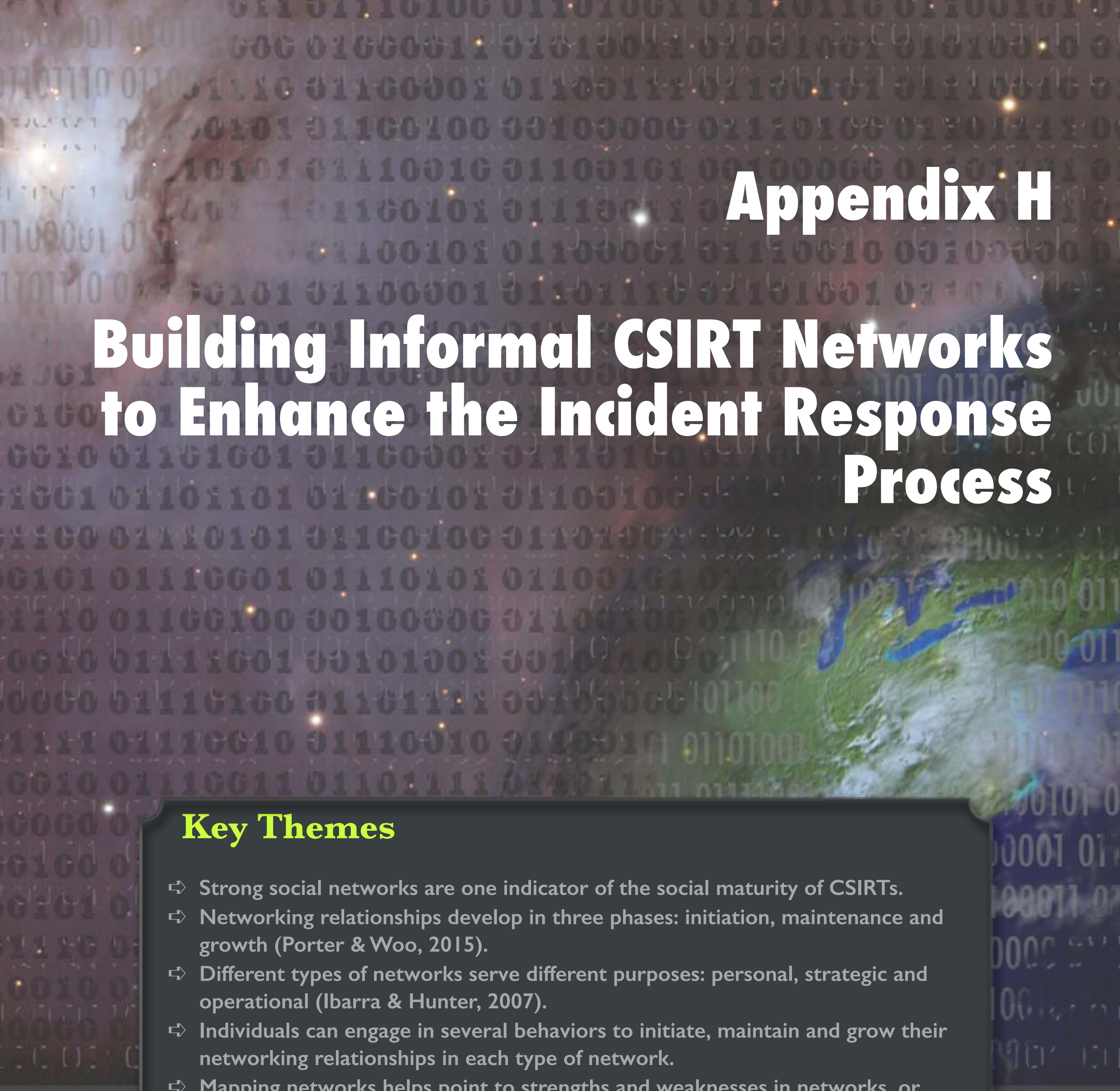
Killcrece, G., Kossakowski, K-P, Ruefle, R., & Zajicek, M. (2003). *Organizational models for computer scurity incident response teams (CSIRTs)* (CMU/SEI-2003-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. http://www.cert.org/archive/pdf/03hb001.pdf

NICE. (2013). The national cybersecurity workforce framework 1.0. Retrieved from http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_interactive.pdf

O*NET; http://www.onetonline.org

Pulakos, E. D., Arad, S., Donovan, M. A., & Plamondon, K. E. (2000). Adaptability in the workplace: development of a taxonomy of adaptive performance. *Journal of Applied Psychology, 85*, 612-624.

Stevens, M. J., & Campion, M. A. (1994). The knowledge, skill, and ability requirements for teamwork: Implications for human resource management. *Journal of Management, 20*, 503-530.



Appendix H

Building Informal CSIRT Networks to Enhance the Incident Response Process

Key Themes

- Strong social networks are one indicator of the social maturity of CSIRTs.
- Networking relationships develop in three phases: initiation, maintenance and growth (Porter & Woo, 2015).
- Different types of networks serve different purposes: personal, strategic and operational (Ibarra & Hunter, 2007).
- Individuals can engage in several behaviors to initiate, maintain and grow their networking relationships in each type of network.
- Mapping networks helps point to strengths and weaknesses in networks, or holes where access to particular resources is missing.
- Leader play a useful role in helping their team members engage in networking, thus increasing team social capital.

Contents

H.1 Acknowledgements

This material is based in part on research sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Homeland Security Advanced Research Projects Agency, Cyber Security Division (DHS S&T/HSARPA/CSD), BAA 11-02 and the Air Force Research Laboratory, Information Directorate under agreement number FA8750-12-2-0258. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

H.2 Target Audience

This white paper summarizes and synthesizes several current models and contributions by organizational scientists who have studied social networking. The primary audience of this paper includes leaders who manage CSIRT teams and/or CSIRT multiteam systems. This paper will be especially useful for CSIRT leaders who seek to expand informal professional networks between their CSIRT and others outside of traditional CSIRT team boundaries (e.g., other cybersecurity professionals in coordinating CSIRTs and formalized groups).

The information in this white paper should be relevant to CSIRTs of all types, sizes, and levels of CSIRT maturity. CSIRT leaders can use information from this white paper to evaluate specific aspects of their CSIRT's maturity, such as those related to the "human" component of many maturity models (NCSC-NL, 2015; Stikvoort, 2010). This information can help them identify ways to enhance social functions of CSIRT teams and team members.

H.3 Introduction

Several maturity models have been introduced to define effective incident handling capabilities of CSIRTs (e.g., documented procedures, appropriate skills among team members) during both routine and novel incidents. CSIRT maturity has been considered "an indication of how well a team governs, documents, performs and measures the CSIRT services" (NCSC-NL, 2015, p. 2). In the maturity model produced by the National Cyber Security Centre in the Netherlands NCSC-NL (2015) five areas of CSIRT maturity are identified (NCSC-NL, 2015, p. 2):

1. **Foundation** – Developing the foundational structure of a CSIRT.
2. **Organization** – Defining and organizing the CSIRT, as well as connecting to the CSIRT community.
3. **Human** – Selecting and training CSIRT members.
4. **Tools** – Creating and choosing automated and essential tools.
5. **Processes** – Establishing and standardizing CSIRT core services.

According to NCSC-NL, the "human" aspect refers to skills and capabilities of CSIRT members. In order to maintain the right skills and capacities, it is suggested that CSIRT members engage in external networking activities to maintain the right social networks.

The "Human" aspect of CSIRT maturity is also described in the SIM3 Maturity Model (Stikvoort, 2010). The SIM3 model describes external networking as "going out and meeting other CSIRTs" and "contributing to the CSIRT system when feasible" (p. 8).

Networking contributes to CSIRT maturity in several ways. One is enabling partnerships between CSIRTs that make it easier to face various cyber-related challenges. Some cyber attacks are too complicated and ambiguous to be managed internally and require additional knowledge that can only be attained from outside resources. Informal relationships also can lead to proactive cybersecurity work that limits the negative consequences of some attacks (e.g., learning of a system defect and fixing it prior to it being compromised). These types of relationships continue to be the focus of many cybersecurity efforts.

In a 3-year effort, our research team created a taxonomy of performance behaviors that effective CSIRT members, teams, and organizations engage in. In order to validate our proposed taxonomy, we conducted 52 focus groups and interviews with over 150 individuals, including CSIRT members, team leaders/managers and leaders of a variety of types of cybersecurity multiteam systems (MTSs). We asked these individuals what behaviors they saw as most important to CSIRT effectiveness. A recurring response was networking behaviors. We were able to identify 64 instances where a CSIRT analyst or leader mentioned the importance of networking.

> **"It's very voluntary and it's – people just tell each other what happened and things that are going on, and well, actually to have such a network is – well, it's a very powerful asset."**
>
> **~ CSIRT Member**

Our findings across various types of CSIRTs suggest that many CSIRT members recognize the importance of networking for effective incident response and supports the assertion that networking is an important human aspect of CSIRT maturity. In order to enhance the human component of CSIRT maturity, CSIRT members should be able to identify the right people to include in their networks, which types of networks will benefit them the most, and how to properly build and maintain different types of networks. We provide these recommendations throughout this paper, as well as recommendations for managers to help their team members build and maintain social networks.

H.4 Networking Defined

The term "networking" refers to specific interactional behaviors that are directed by individual, team, or organizational goals (Gibson, Hardy, & Buckley, 2014). These behaviors can occur both inside and outside of an organization and are aimed at gaining interpersonal resources (Gibson, et al., 2014; Porter & Woo, 2015) by developing relationships with others whom are viewed as helpful to one's work or career (Forret & Dougherty, 2001). According to Wolfe and Moser (2009), networking *behaviors* often serve one of three purposes: building, maintaining or using contacts (we offer strategies for each below). Accordingly, Porter and Woo (2015) argued that networking relationships develop in three stages, characterized by the depth of the relationship and quality of exchanges between partners. In the first stage, *initiation*, networking behaviors involve introductory exchanges between potential contacts. These exchanges represent each party providing the other with universally helpful resources, which reveals information about the usefulness of each party. For example, one partner may be able to determine if the other has access to a valued resource by gleaning information such as where they work, the knowledge and skills they have, or how much social capital they can offer (other personal connections they may have). If both parties decide the other is useful, then, according to Porter and Woo, the relationship enters the *growth* stage where the focus is on strengthening the relationship. Exchanges in this stage aim to increase perceptions of trustworthiness of each partner, as each partner keeps their promise to provide useful resources to the other. For example, one party might ask the other for a particular favor, and then provide something in return. These actions demonstrate integrity on behalf of both partners. Finally, Porter and Woo propose that the relationship continues into the *maintenance* stage, where further networking interactions are conducted to develop a high-quality relationship. High-quality exchanges in this stage involve integrity (keeping one's word) and acting in one another's best interests (Porter & Woo, 2015).

> **"What you see, especially with my network, which is more external, trusted security groups, for example, law enforcement, secret service, all different kind of people that work with cyber crime that you can somewhat trust, and they come together as well in a structured way. Every year at least we get together, shake hands, exchange knowledge… and the best thing you can do is just go, sit or stand at the podium and give a presentation. That is the quickest way to build a network because people come to you."**
>
> **~ CSIRT Member**

Acquiring networking relationships increases a person's social capital, (Forret & Dougherty, 2001). The more connections a person has in their social network, the greater their social capital. Social capital is a valued resource, as it allows individuals access to information, opportunities and other resources that can aid in accomplishing

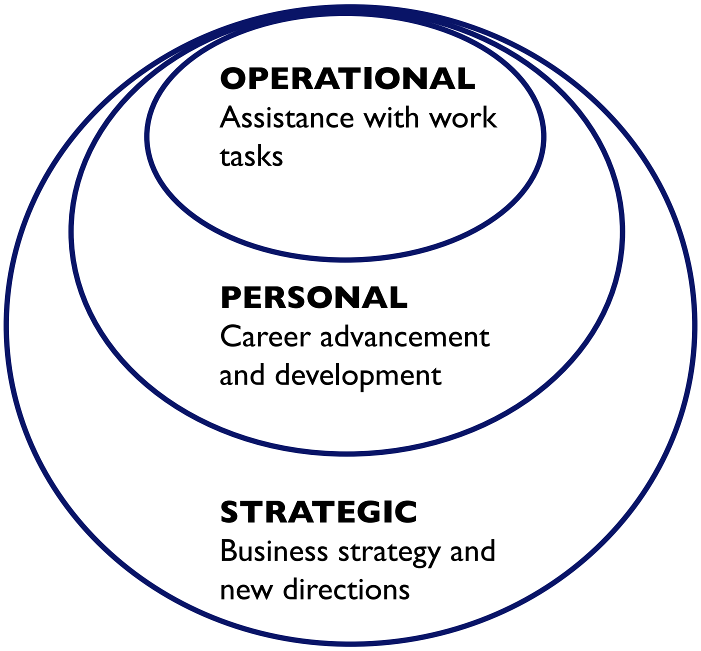

OPERATIONAL
Assistance with work tasks
PERSONAL
Career advancement and development
STRATEGIC
Business strategy and new directions

Figure H.1 Types of networks that influence CSIRT functions (Ibarra & Hunter, 2007).

work tasks or managing one's career (Forret & Dougherty, 2001). By facilitating network development among their team members, CSIRT managers can enhance the social maturity and effectiveness of their employees and teams (Uzzi & Dunlap, 2005) CSIRT members will gain increased access to information and diverse skill sets, as well as power (the ability to influence). Individuals who successfully network also demonstrate higher levels of career success (Wolff & Moser, 2009) and job performance (Thompson, 2005).

Different network contacts can be useful in different ways. For example, some contacts may be maintained or used to help with career mobility, while others might have access to useful information that helps with a work objective. For this reason, different types of networks have been identified that can be utilized according to one's particular needs.

H.5 Types of Networks

Ibarra and Hunter (2007) identified three types of networks that individuals should develop and maintain are displayed in Figure H.1 (Ibarra & Hunter, 2007). These three types of networks – *operational, personal*, and strategic -- help provide those who use them with resources, information, insight, feedback, and support. In cybersecurity work, which involves many technical and analytical tasks that are completed by teams, networks add a vital relational component that expands social capabilities of team members, and therefore, the CSIRT (Forret & Dougherty, 2001).

Operational Networks. Operational networks help CSIRT members manage cybersecurity-related work tasks. These networks can be comprised of members of the same team or cybersecurity multiteam system (MTS; multiple teams who work together closely), individuals within the organization who provide support for a project (e.g., legal teams), or key stakeholders outside the organization, such as cybersecurity personnel in other companies, or national/coordinating CSIRTs. These networks are useful because they rely on coordination, cooperation, and trust among parties in order for the task at hand to be completed effectively. Any CSIRT with operational functions should encourage their members to develop operational networks.

Personal Networks. Personal networks are comprised of individual relationships that boost individual development. They often serve the purpose of advancement of the party in question (e.g. career management or job search; Porter & Woo, 2015). Personal networks can be beneficial sources of referrals and support, such as coaching and mentoring (Ibarra & Hunter, 2007). External contacts have the ability to provide recommendations and referrals to others outside of any existing networks. Development of personal networks enables the exploration of new ideas and leads to the development of new connections with others.

Strategic Networks. Strategic networks help identify directions for business approaches and stakeholders, similar to the way Clark et al. (2014) suggest National Cyber Security Centers promote strategic cybersecurity development. Strategic networks extend beyond operational networks because they are centered on business functions rather than operational functions (Ibarra & Hunter, 2007). These types of networks help CSIRTs distinguish themselves from others because they help members identify valuable sources of information and other resources. For example, CSIRT members can engage in any of numerous cybersecurity related forums or build relationships with outside groups (e.g., academics, ISACs) that promote collaboration, knowledge sharing, education and training among public and private sector cybersecurity professionals. By helping their team members to develop both personal and operational networks in a strategic fashion, CSIRTs managers can accentuate their teams' abilities to seek out appropriate conversations and resources.

H.6 Development and Maintenance of Networks

Networking behaviors are "aimed at building, maintaining, and using informal relationships that possess the (potential) benefit of facilitating work-related activities of individuals by voluntarily granting access to resources and maximizing common advantages" (Wolff & Moser, 2009, p. 196-197). Researchers have identified five specific networking behaviors: engaging in social activities (e.g., attending functions with coworkers outside of work), engaging in professional activities (such as attending conferences), being involved in the community (e.g., church, sports, or clubs), being engaged internally at work (e.g., inviting a superior to lunch), and maintaining and increasing contacts (Forret & Dougerty, 2004, Ibarra & Hunter, 2007; Thornton, Henneberg & Naude, 2013, Wolff & Moser, 2009) . These behaviors can lead to the identification of contacts that can be utilized for career purposes, for personal development, for help with work tasks when contacts are within the organization, or for identifying strategic directions. Often, establishing personal connections can provide the foundation for strategic and operational connections. Certain types of behaviors can also aid in maintaining the networking relationship once initial contact has been made and both parties find one another to possess valuable resources for one of more of their needs. As CSIRTs are often involved in handling novel or complex incidents, operational and strategic networks are vital for bringing together various experts and skill sets needed to create a novel solution. Having contacts with unique experiences and expertise to call on can make this process much more efficient. Additionally, strategic and operational networks can increase knowledge development and learning in the organization (Faraj & Yan, 2009). Having contacts outside the organization in a similar industry or in the cybersecurity world can also help CSIRTs be proactive in preventing attacks when members of different organizations trust one another and share important information. In this way, both parties are exchanging valuable resources that can be mutually beneficial.

H.6.1 NETWORK MAPPING

As it can often be challenging to identify the right people to include in one's network, or to keep track of who has what resources, several worksheets and webpages exist for mapping out social networks. For example, the website www.mindtools.com offers several exercises to help identify specific sources of support. In one exercise, individuals can consider 14 different sources of support, what resources those sources can offer, and what they might expect in return. Identifying network contacts that fill these categories can bring to light any gaps or holes one may have in their networks. By identifying the types of connections that already exist, people can identify the connections that would be most beneficial for them to make. It is advised that individuals aim for a blend of people with similar experiences and training to their own, as well as a diversified network of individuals (Uzzi & Dunlap, 2005). Including individuals of different nationalities and with differing world-views can be beneficial in initiating innovative ideas. Leaders can help their team members initiate new contacts by engaging in high-stakes activities that connect team members to others they would not usually connect with. Shared activities enable disparate entities to find a common point of interest and allow those involved to break free from typical patterns of behavior.

H.6.2 NETWORKING IN WORK TEAMS

Thus far, we have elaborated on networking to increase individuals' social capital, but social capital can be assessed at the team level as well. The more social capital individual members have, the greater the social capital of the team as a whole (Marrone, 2010). In order for work teams to maintain useful operational and strategic networks, as well as increase the number of relationships within them, team members in the CSIRT must engage in boundary management within and outside of the organization. Managing boundaries increases the team's access to needed information, stakeholder perceptions of team performance, perceptions of psychological safety, and overall team effectiveness (Allen, 1984; Druskat & Wheeler, 2003; Faraj & Yan, 2009; Guinan, Cooprider, & Faraj, 1998; Tushman, 1977; Zmud, 1983). *Boundary spanning* is typically the way in which between-team boundaries are managed and helps teams accomplish their objectives. Boundary-spanning is characterized by activities such as building external relationships, scouting for and attaining available resources (e.g., information), gaining support for the team, and championing or promoting the team's work (Druskat & Wheeler, 2003; Faraj & Yan, 2009). Boundary spanning activities can promote the development of operational and strategic networks by helping the team (and those connected to the team) complete task objectives and achieve performance goals (Marrone, 2010).

One person within a team usually acts as the team's point-of-contact ("boundary spanner") with other teams or parties by coordinating communications (Marrone, 2010). This person can utilize his or her own or the entire team's strategic and operational network contacts to ask for assistance with incident management, inquire about important information, remain in the loop about organizational developments, gain project specific expertise, or for other purposes. Boundary spanners bring additional resources to the team while simultaneously developing both personal and team-wise networks (Marrone, 2010).

Team leaders can benefit their teams by identifying the current status of their team's network, including potential "connectors" who are likely to be more fully engaged in boundary spanning activities (Ibarra & Hunter, 2007). They can then provide these "connectors" with direction and guidance for building relationships (see Table H.1). Leaders can facilitate network development by encouraging team members to reach out to others or by introducing them to potential connections (Ibarra & Hunter, 2007). These behaviors can especially help those who may not know

TABLE H.1 LEADER BEHAVIORS TO INFLUENCE NETWORKING (ADAPTED FROM IBARRA & HUNTER, 2007)

LEADER NETWORKING RECOMMENDATION	ACTIVITIES INVOLVED
Adjust your mindset	• Allocate enough time and effort for networking to be successful • Role model networking activities for team members • Provide feedback to team members about their networking activities
Find common ground with potential partners	• Use personal interests strategically (e.g., take clients to events that enable you to learn about their interests) • Use functional interests and expertise to reach out to others that can contribute to your knowledge development
Manage your time	• Continue to practice networking to remain effective at it • Engage in informal discussion with several people to gather needed information. • Network continually to keep this information up-to-date
Be proactive	• Do not wait until you need something- pick up the phone at every opportunity • Keep your network alive by using it often • Connect people whom you think should meet
Be Patient	• Keep working at it-networking requires continued practice • Build networks such that they cross both organizational and functional boundaries and then link them together in new ways • Accept that rewards of networking take time and are often delayed.

who to reach out to. Leaders can help establish potential connections by identifying common ground between individuals (Ibarra & Hunter, 2007). Often, personal interests can be transposed into strategic goals. Engagement in activities related to personal interests (e.g., simply having a beer after a conference meeting) can prove beneficial, as conversations held during such activities can provide insights into how each party functions or allow for the identification of functional interests that build relationships and new knowledge (Ibarra & Hunter, 2007). Leaders should also encourage networking behavior even in the absence of a specific need. Successful networkers invest time and effort into maintaining relationships whether it be to receive assistance, provide assistance, give feedback, or simply communicate (Ibarra & Hunter, 2007).

H.7 Conclusion

Effective CSIRTs are comprised of people and teams with strong personal, operational and strategic networks- a component of CSIRT maturity. Those networks are built by communicating and connecting with individuals, teams, and other parties through a number of activities identified in this paper and by initiating, maintaining and growing fruitful exchange relationships (Porter & Woo, 2015). Building of different types of networks results in enhanced performance and innovation, among other benefits, by increasing access to resources that both individuals and teams can utilize. Networks rich in diverse contacts also aids in individual development and career advancement (Porter & Woo, 2015). By understanding the function of networking and the purpose each type of network serves, individuals can then map out their networks and identify the resources they have and those they still need (Uzzi & Dunlap, 2005). Leaders can play a helpful role in establishing connections and providing resources to their teams by encouraging networking behaviors and providing guidance. Research indicates that the ability to enlist the appropriate people and groups necessary for the development of a team's vision is what distinguishes leaders from managers (Ibarra & Hunter, 2007).

References

Allen, T. J. (1984). *Managing the flow of technology*. Cambridge, MA: MIT Press.

Druskat, V. U., & Wheeler, J. V. (2003). Managing from the boundary: The effective leadership of self-managing work teams. *Academy of Management Journal, 46*(4), 435-457.

Faraj, S., & Yan, A. (2009). Boundary work in knowledge teams. *Journal of Applied Psychology, 94*(3), 604.

Forret, M. L., & Dougherty, T. W. (2001). Correlates of networking behavior for managerial and professional employees. *Group & Organization Management, 26*(3), 283-311.

Forret, M.L. & Dougherty, T.W. (2004). Networking behaviors and career outcomes: Differences for men and women? *Journal of Organizational Behavior, 25*, 419-437.

Gibson, C., Hardy III, J.H., & Buckley, M.R. (2014). Understanding the role of networking in organizations. *Career Development International, 19*(2), 146-161.

Guinan, P.J., Cooprider, J.G., & Faraj, S. (1998). Enabling software development team performance during requirements definition: A behavioral versus technical approach. *Information Systems Research, 9*(2), 101-125.

Ibarra, H. & Hunter, M. (2007). How leaders create and use networks. *Harvard Business Review*, 40-47.

Marrone, J. A. (2010). Team boundary spanning: A multilevel review of past research and proposals for the future. *Journal of Management, 36*(4), 911-940.

National Cyber Security Centre, The Netherlands, 2015. "CSIRT Maturity Kit - A step-by-step guide towards enhancing CSIRT Maturity." Paper written for the Global Conference on Cyber Space 2015, 8 Apr. p. 2. https://www.gccs2015.com/sites/default/files/documents/CSIRT%20Maturity%20Toolkit%2020150409.pdf.

Porter, C.M. & Woo, S.E. (2015). Untangling the networking phenomenon: A dynamic psychological perspective on how and why people network. *Journal of Management, 41*(5), 1477-1500.

Stikvoort, D. (2015). SIM3: Security Incident Management Maturity Model. *Trusted Introducer, 30*.

Thompson, J. A. (2005). Proactive personality and job performance: A social capital perspective. *Journal of Applied Psychology, 90*, 1011–1017.

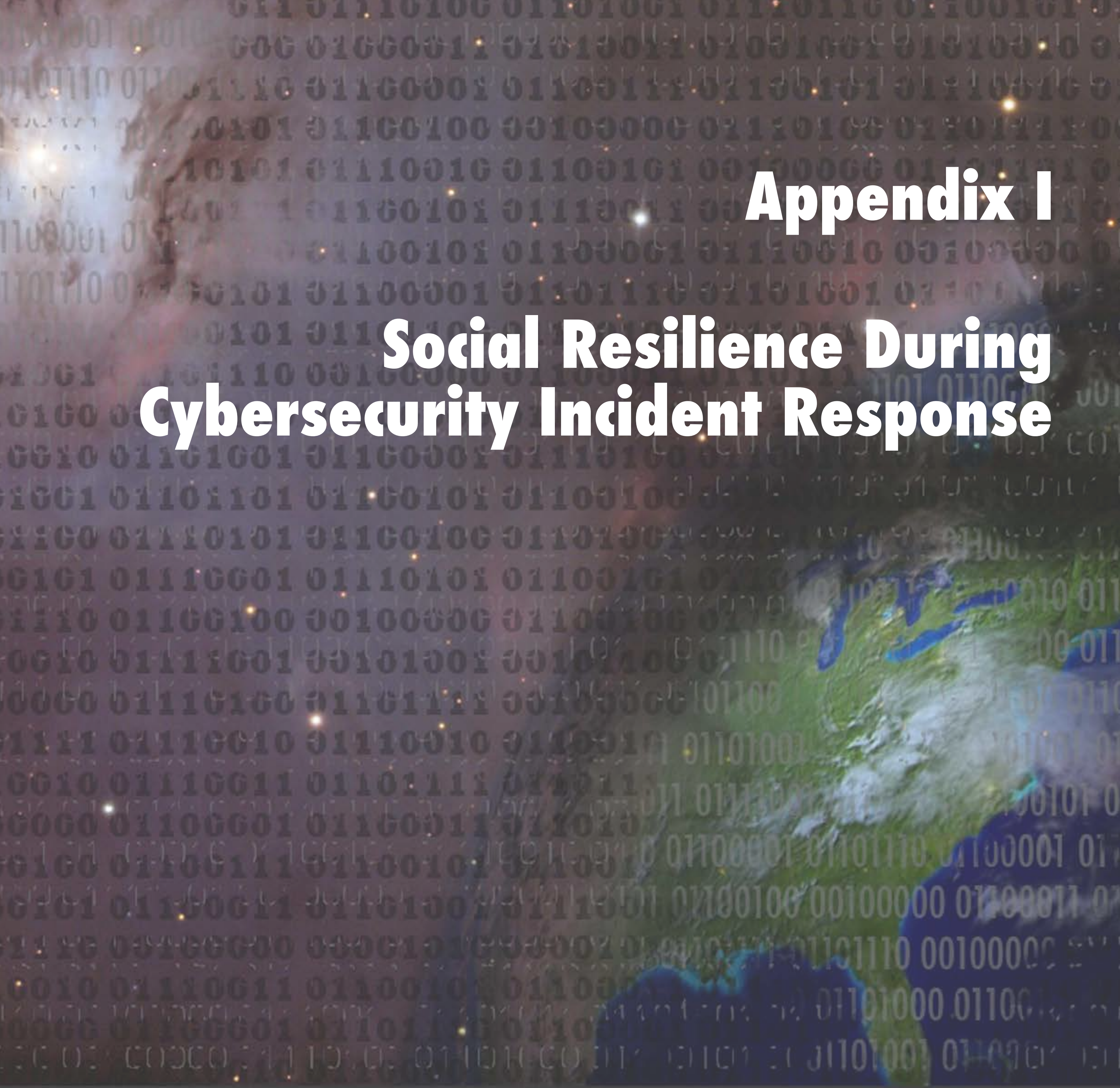
Thornton, S.C., Henneberg, SC. & Naude, P. (2013). Understanding types of organizational networking behaviors in the UK manufacturing sector. *Industrial Marketing Management, 42*(7), 1154-1166.

Tushman, M. L. (1977). Special boundary roles in the innovation process. *Administrative Science Quarterly*, 587-605.

Uzzi, B. & Dunlap, S. (2005). How to build your network. *Harvard Business Review*.

Wolff, H.G. & Moser, K. (2009). Effects of networking on career success: A longitudinal study. *Journal of Applied Psychology, 94*(1), 196-206.

Zmud, R. W. (1983). The effectiveness of external information channels in facilitating innovation within software development groups. *MIS quarterly*, 43-58.



Appendix I

Social Resilience During Cybersecurity Incident Response

Contents

1.1 Purpose

Cybersecurity incident response teams (CSIRTs) function within complex environments that have potentially negative impact on incident mitigation. When stress is too high in intensity or duration, CSIRTs must adapt to a variety of stressors as quickly as possible in order to maintain or recover from adversity. Adaptation or recovery from adversity is known as resilience (Alliger, Cerasoli, Tannenbaum, & Vessey, 2015). Although many CSIRTs focus their attention on maintaining the resilience of technical systems they support, attention to how adversity and stress affects the individuals and teams who interact with technical systems could play a vital role in maintaining overall effective functioning of CSIRTs. We refer to this focus as social resilience (i.e., the psychological resilience of individuals and the teams in which they function; Cacioppo, Reis, & Zautra, 2011). Although research is lacking on the interplay between technical and social resilience (i.e., how one influences the other), decreased performance of either technical systems or the people who build, run, and maintain those systems can greatly impact the ability of the broader system to remain functional. The purpose of this white paper is to help CSIRT leaders understand and develop individual and team resilience as it applies to the cybersecurity domain. CSIRT managers who understand these forms of resilience will be able to:

- Understand aspects of social resilience, such as individual and collective (team) resilience;
- Identify factors that impact an individual's ability to demonstrate resilience;
- Identify factors that impact a team's ability to demonstrate resilience; and
- Implement various strategies to maintain and enhance individual and team resilience among their CSIRT members.

Throughout this white paper, best practices from the field of organizational psychology are provided that are known to affect individual and team resilience. By understanding the impact that stress can have on individual and team functions, CSIRT managers can attempt to manage such sources of stress and assist their team members in ways that mitigate the potentially negative consequences associated with stressful demands during the incident response process.

1.2 Target Audience

This white paper summarizes and synthesizes several current models and contributions by organizational scientists who have studied resilience. The primary audience for this paper includes leaders who manage CSIRT teams and/or CSIRT multiteam systems. CSIRT multiteam systems (MTSs) refer to a tightly coupled network of teams that work closely together to resolve incidents (DeChurch & Marks, 2006). This paper will be especially useful for CSIRT leaders who seek to understand how stress associated with the incident response process can affect CSIRT performance.

The information in this white paper should be relevant to CSIRTs of all types, sizes, and levels of CSIRT maturity. CSIRT leaders can use information from this white paper to identify ways to help their teams maintain effective functioning within CSIRTs and individual members. Enhanced focus on the social resilience of CSIRTs could benefit some aspects of their CSIRT's social maturity (see Chapter 2 on the social maturity of CSIRTs).

1.3 Introduction

Cybersecurity incident response often occurs within complex and adaptive settings that involve working under stressful and challenging conditions. Although at times, these conditions might have positive effects on cybersecurity professionals (e.g., stress can motivate them to work harder or seek new resources), when incident response becomes overly stressful in terms of duration or intensity, the outcome can be a drop in performance (e.g., systems remain vulnerable, mistakes are made). Effective CSIRTs demonstrate one of two capabilities during incident response management: a) performance is maintained, most often by successfully adapting to new demands associated with stress, or b) they suffer an initial loss in performance, but recover and sometimes even increase their performance in the process of doing so. Both of these circumstances reflect resilience: the ability to withstand or recover from adversity (Alliger, et al., 2015; Richardson, Neiger, Jensen, & Kumpfer, 1990). Interestingly, most references to cybersecurity resilience refer to the resilience of only technical systems and do not consider resilience of the social systems (i.e., individuals and teams) behind technical capabilities. This white paper focuses on the role of individual and team resilience in cybersecurity work from a psychological perspective. In the following sections, we review why resilience of the social systems involved in cybersecurity incident response should be considered and provide an overview of individual and collective (e.g., team) resilience. We conclude with suggestions regarding the development of resilience among CSIRTs and their team members.

1.4 Why Resilience Matters in Cybersecurity

As outlined in Chapter 1 ("Introduction to the Handbook"), the nature of CSIRT work involves functioning in volatile, uncertain, complex, and ambiguous (VUCA; Stiehm, 2010) environments that require CSIRT members to effectively work while stressed. CSIRT members demonstrate resilience when they effectively manage the stress that arises in such environments. However, the incident response process is sometimes lengthy and intense, resulting in many negative effects of stress on CSIRT performance.

1.4.1 THE IMPACT OF STRESS

As events such as cyber-attacks arise, individuals and teams can experience high levels of stress that test their ability to perform

“It’s 2:00 in the morning, and you want to go to sleep. And you can’t because you’ve got to make sure that all the different aspects of that particular incident is taken care of, containment and making sure you scope, and all those sorts of things. And you may not be able to get in touch with someone. But yet, it’s still an incident. And you don’t have an understanding of the impact of the incident. But it’s 2:00 in the morning, so you’ve got to figure out a way to work with other people. Maybe take shifts, do a lot of different things that require you to be resilient. It’s just not a ‘hey, what’s written on paper is the way it’s going to be’. That’s not how it is.”

under pressure. Stress can stem from objective sources, such as intense workloads (e.g., dealing with multiple incidents), or prolonged exposure (e.g., long-duration attacks). Perceptions of stress also can differ among individuals. For example, Lazarus and Folkman (1984) found that some individuals view stressful circumstances as challenges, while others view stress as threats, although those who view stress as a challenge tend to use more successful coping strategies (Folkman & Moskowitz, 2004).

These effects can impair not only the job performance of CSIRT members, but also their mental and physical well-being. Individuals who face high job demands can experience symptoms of burnout (e.g., emotional exhaustion), sleep problems, digestive issues, or other signs of impaired well-being (De Lange, Taris, Kompier, Houtman, & Bongers, 2004; Maslach, Schaufeli & Leiter, 2001; Warr, 2007). Continuous job demands also result in decreased energy levels that can result in a “loss spiral” when individuals find it difficult to stay engaged with their work and lack the resources to recover, further succumbing over time (Hobfoll, 2001, p. 354; Hobfoll & Lilly, 1993). As these problems persist, individuals face increased risk for health problems and disengagement from their jobs that might lead them to seek other employment (Schaufeli & Bakker, 2004). Even those who remain in their jobs might experience “cutback days” where, despite being present for work, they demonstrate decreased performance (Flaxman & Bond, 2010, p. 345; Hardy, Woods, & Wall, 2003).

Exposure to prolonged or intense stress also impacts team processes. When teams (or individuals within those teams) experience stress, team interactions can become less effective. For example, continuous stressors such as ambiguous team roles or interpersonal conflicts can decrease team cohesion and performance (Alliger, Cerasoli, Tannenbaum, & Vessey, 2015). Additionally, as stress increases, individuals tend to rely less on other team members’ knowledge and expertise (Driskol, Salas, & Johnston, 1999; Ellis, 2006), thereby resulting in increased mistakes and decreased team performance. High team stress not only impacts team performance, but also can inhibit team learning as well, ultimately resulting in increased workloads that also prove detrimental to individual performance (Savelsbergh, Gevers, van der Heijden, & Poell, 2012).

It is important that individuals and the teams they work in are able to adapt to new challenges and effectively manage the stress that comes with those challenges. Adaptable individuals and teams can learn more from their experiences, which helps them prepare for future ambiguous circumstances (see Chapters 1, 5, 7, and 11 for information on adaptation). However, when successful adaptation is not possible, individuals and teams must be able to recover from any performance decrements as soon as possible to remain effective. An organization’s ability to quickly recover from cyber-attacks is paramount to organizational success and can even impact an organization’s ability to remain in existence. Cyber-attacks can impact a variety of organizational aspects, including production and customer relations. Many of these aspects ultimately influence organizational finances, resulting in clear costs associated with cyber-attacks.

The Financial Impact of Stress due to Cyber Attacks

Cyber-attacks often substantially impact businesses’ finances. Responses from the 2013 Global Corporate IT Security Risks Survey (Kaspersky Lab, 2013) estimate the average cost of a cyber-attack on large companies to be $649,000, with average loss figures of $818,000 in North America and $627,000 in Western Europe (The high cost of a security breach, 2013). The consequences of very severe cyber-attacks can be even worse, as was the case for DigiNotar in 2011, which filed for bankruptcy about one month after the discovery of an attack (Keizer, 2011).

Adaptation to financial loss due to cyber-attacks is most likely not an option for many businesses. Thus, it often is paramount that businesses recover from the financial effects of cyber-attacks as quickly as possible. Enhancing the social resilience of CSIRTs enables organizations to potentially mitigate losses (financial and otherwise) associated with cyber-attacks.

In the next section, we review the concept of social resilience and describe characteristics of resilient individuals and teams. Research indicates that these characteristics help individuals and teams to either maintain their abilities in the face of adversity or recover quickly from stressful experiences, thereby lessening the potential negative effects of stress

I.4.2 SOCIAL RESILIENCE IN CYBERSECURITY

CSIRT leaders need to manage individual and collective (team) responses to stress – the resilience of the social system. Researchers (e.g., Britt & Jex, 2015; Zaccaro, Weiss, Hilton, & Jeffries, 2011) have suggested that resilient individuals and teams demonstrate consistent characteristics and actions.

Factors that reflect social resilience include individuals' personal attributes (e.g., personality traits), abilities to engage in effective problem-solving, use of effective coping skills, or the ability to seek out potentially helpful resources such as social support networks. Social resilience is also impacted by the extent to which teams can maintain and carry out effective team processes that center around cohesion and communication, among others.

Table I.1 summarizes aspects of social resilience that are likely to be evident among CSIRTs as a result of enhanced individual and team resilience. These aspects include individual and team characteristics that research suggests serve as precursors to resilience (i.e., individuals or teams demonstrating these characteristics also tend to demonstrate resilience), as well as behavioral actions that resilient individuals and teams tend to engage in. The last column of the table includes the results of these characteristics and behaviors (i.e., resilient outcomes) in the face of stress and adversity. Several of these characteristics and behaviors are reviewed in the following sections

INDIVIDUAL RESILIENCE

Research on resilience at the individual level tends to focus on three aspects: personality traits (e.g., optimism, hardiness, and self-efficacy), social support, and coping/problem-solving skills (see Figure I.1). Many of these aspects (e.g., personality traits) are considered to be individual characteristics that serve as precursors to an individual's ability to be resilient. In other words, resilient individuals often demonstrate many of these personality traits (Garmezy et al., 1984). Other aspects reflect actions that many resilient individuals engage in when reacting to stress and adversity.

PERSONALITY TRAITS

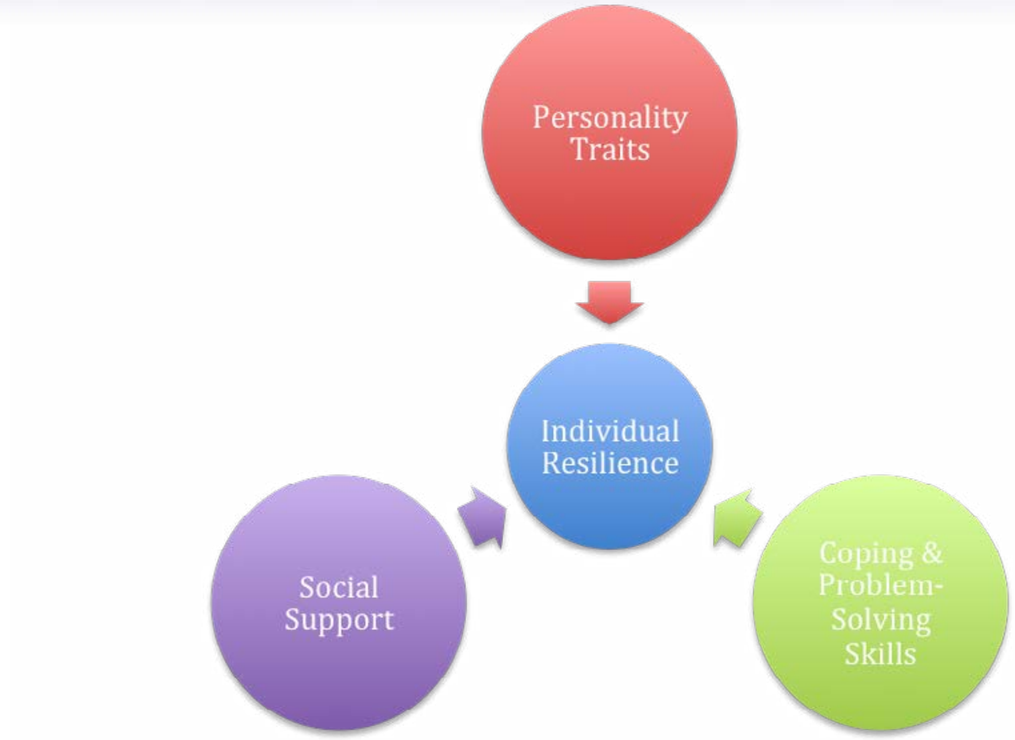
Individuals vary in characteristics that influence how they view and react toward stress and adversity. Personality traits are considered to represent relatively stable aspects that reflect individuals' reactions across a variety of settings and circumstances. Although personality traits are considered stable over time, they can be influenced, to some extent, by circumstances in the environment, and in some occasions, dysfunctional aspects of personality can be altered with treatments such as psychotherapy (Magnavita, 2004). Many personality traits have been researched in connection with individual resilience in an effort to determine what "type" of individual is likely to react to stress in ways that limit any potentially negative effects. A meta-analysis by Connor-Smith and Flachsbart (2007) reported that different personality traits related to the use of various coping strategies that minimize negative reactions to stress and adversity. Common personality factors that provide the dispositional basis for individual resilience include optimism, self-efficacy, and hardiness, among others.

Dispositional Optimism. An individual's tendency to be optimistic can influence his or her expectations about an events' outcome. Dispositional optimism, that is, the expectation of a positive outcome, is considered by some researchers to be a characteristic that helps individuals cope with stress (Garmezy et al., 1984; Maddi, 2002, 2004; Maddi & Kobasa, 1984). CSIRT analysts who expect positive outcomes, such as being able to effectively mitigate an incident, might experience lower levels of stress throughout the incident response process, and be able to direct resources to the task at hand. On the other hand, individuals with less positive expectations about their ability to manage an incident might feel increased pressure because they

TABLE I.1 ASPECTS OF SOCIAL RESILIENCE

LEVEL	CHARACTERISTICS	ACTIONS	OUTCOMES UNDER STRESS
Individual (Employee)	• Optimism • Hardiness • Belief in one's ability (self-efficacy)	• Seek out social support when stressed • View stress as a challenge rather than a threat • Use of problem-focused coping skills • Engaged in problem-solving activities	• Mental health • Physical well-being • Sustained or improved job performance • Sustained or improved relationships
Collective (Team or Multiteam System)	• Collective belief in the team's capabilities (collective efficacy) • Empowered team members • Clear understanding of team roles	• Seek resources through social networks • Demonstrate satisfaction with their work • Provide backup assistance • Develop and use standard operating procedures	• Sustained or improved team processes • Sustained or improved resource networks • Sustained or improved team effectiveness and performance

Figure I.1 Factors that compose individual resilience.



focus on problems that might arise from failure, rather than focusing on the response process itself. Under these circumstances, CSIRT analysts who focus on problems potentially waste valuable cognitive resources and distract themselves from potential solutions, thereby decreasing other resources (e.g., energy) that could be directed at the task. Individuals also should be aware of the extent to which their optimism surrounding their abilities to resolve incidents reflects overconfidence rather than optimism. Overconfidence in one's ability can result in confirmation bias (i.e., seeking information that confirms a specific point of view) or the expectation that decisions are more accurate than they might be (Heath, Larrick, & Klayman, 1998; Russo & Schoemaker, 1992). We refer readers to Chapter 4 ("Decision-making in CSIRTs") for more information on this topic).

Hardiness. Individuals who demonstrate the personality trait of hardiness tend to be less affected by stress and adversity and more likely to cope with stress than less hardy individuals (Kobasa, 1979; Maddi, 1999). Hardy individuals demonstrate high levels of three factors: control, commitment, and challenge (Kobasa, 1979). Individuals with a high sense of control believe they can take action on various aspects of their lives. Hardy individuals also tend to be committed to things that matter to them and to view stressful circumstances as challenges rather than threats. Individuals can develop their hardiness through a training program described at the end of this paper.

Self-Efficacy. Psychologists (e.g., Bandura, 1997) refer to individuals' beliefs that they can carry out specific actions or behaviors as self-efficacy. Individuals with high levels of self-

> **“I was on a couple past large breach investigations and just the management styles on both teams were completely different. One of them was, I mean it was a very high stress environment for them. But not at any time did they reflect that on the SOC or the SIRT team. So that really kept us from being able to stay calm and work in environment without going crazy. But on the other hand another engagement was completely different. The management style was just totally stress, stress, everything was high stress. And it put a lot of pressure on the teams. I mean in some cases it really had a negative impact on the performance. So that's a really excellent point, management and the way they kind of deal with it has a definite effect on the team.”**

> **“I have always looked for grit, like personal resiliency, because I think this is an environment – we’re in a role where we only ever really deliver bad news. Well, pretty much, we only ever hear bad news… The Internet has inoperable cancer again. And we have to tell everybody that the Internet is broken, and there’s no two ways around it… Get rid of that thing that you have come to rely upon. It’s like ‘so much for those baby pictures, you definitely caught crypto blocker and you should have had backups.’ All those sorts of things, I think that requires a certain degree of good resiliency to be able to deal with that… And also, just the general environment is very dynamic. There is political pressure from time to time… people without those qualities I think are not likely to spend a great deal of time doing this part of the work in this environment. So that’s what I generally look for, as one of the primary qualifications.”**

efficacy, those who believe they possess the ability to successfully complete a specific action, are more problem-focused compared to individuals who lack confidence and respond with greater emotion (Jex & Bliese, 1999). When training individuals, those low in self-efficacy tend to prefer more formalized training compared to high self-efficacy individuals who are more comfortable with situations where role requirements might be ambiguous or there is greater opportunity for error (Jex & Bliese, 1999). In a study of U.S. Army soldiers by Jex and Bliese (1999), lower levels of self-efficacy were associated with higher levels of physical and psychological strain and lower levels of job satisfaction and organizational commitment. Even under circumstances where workload was high, individuals who believed in their abilities to be successful at work experienced lower levels of stress. However, the same caveat regarding the potential for overconfidence mentioned earlier should be considered here as well. In regard to both optimism and self-efficacy, CSIRT managers might be better served by helping team members who demonstrate lower levels of these personality traits focus more on learning to improve their outlooks in different circumstances rather than seeking highly optimistic and self-efficacious (and potentially over-confident) individuals.

Personality provides a dispositional basis for individual resilience. However, various training programs can help individuals adjust their behaviors by helping them recognize how their thoughts influence subsequent behaviors. For example, although people might possess the general tendency to focus on problems rather than solutions (i.e., demonstrate a lack of optimism), training in cognitive methods can help people learn to identify these tendencies (Liossis, Shochet, Millear, & Biggs, 2009). Once learned, people can then catch themselves focusing on the problem and attempt to reframe problems in a positive, optimistic light that might help guide future actions (e.g., focus on what to do next rather than complain about the problem). We review practices that can help individuals develop resilient tendencies in a later section.

SOCIAL SUPPORT

The collaborative nature of cybersecurity incident response results in individual team members seeking help and support from other team members. Social support helps individuals deal with the demands of stressful circumstances, thereby enhancing their ability to demonstrate resilience (Britt & Jex, 2015). Beehr (1995) identified two important aspects of social support: the source from which social support is received, and the type of social support provided. Common sources of social support include peers and coworkers, supervisors, and significant others (e.g., family, spouses and friends). The type of resources that various sources of social support can offer to the individual in need impacts the effectiveness of social support. For example, if an analyst were overworked, only his or her supervisor would have the ability to approve additional time off. The type of social support provided can be either tangible, instrumental support that helps the person manage stress (e.g., a coworker helping to cover the workload of an overworked colleague), or emotional support in the form of listening, offering encouragement or advice to someone who is stressed (Britt & Jex, 2015). CSIRT managers could benefit their team members by encouraging them to develop strong social networks that either provides valuable resources or emotional support during times of stress (we refer readers to Appendix H for more information). CSIRT managers also can benefit their team members by encouraging cooperation and collaboration within their team rather than a sense of competition. They can do this by having team members focus on overall team goals and implementing team reward structures (Britt & Jex, 2015).

COPING AND PROBLEM-SOLVING

Individuals react to stress by using various coping strategies, although some strategies are more effective than others. Effective coping skills can help people react to stress in ways that make them more resilient by providing them with experience and knowledge that can be useful in similar stressful situations. Researchers have identified two categories of coping methods: emotion-focused and problem-focused coping methods (Britt & Jex, 2015). Emotion-focused strategies aim to eliminate or lessen negative feelings associated with stress. For example, a CSIRT analyst might feel overwhelmed while handling an attack on a financial database because of the increased stress that results from potentially losing

TABLE I.2 MANAGER ACTIVITIES TO ENCOURAGE EFFECTIVE COPING OF TEAM MEMBERS (ADAPTED FROM BRITT & JEX, 2015)

MANAGER ACTIVITY	EXAMPLES
Model effective coping behaviors	• Take breaks yourself and remind team members to do the same • Focus on the identification of problem-solving strategies rather than complaining without offering a solution
Encourage openness about stressful experiences at work	• Allow time for identification and discussion of stressful events during meetings
Enhance awareness of organizational resources among team members	• Post information related to available resources in highly visible areas • Refer or remind stressed team members of specific resources

vast amounts of financial data. The analyst might choose to eliminate stress by deciding to take a coffee break to chat with others not involved in the incident. Although this response might help the CSIRT analyst feel better by taking him or her away from the stressful incident, it does not solve the problem of the attack itself. Therefore, a downside associated with emotion-focused coping methods is that they do not do anything to actually mitigate the source of stress, although sometimes it is helpful for an individual to express feelings related to a problem before tackling the problem (Britt & Jex, 2015). In some cases, people can choose potentially negative coping strategies (e.g., drinking too much) that might decrease stress temporarily but could result in long-term damage (e.g., addiction).

Problem-focused coping methods, on the other hand, focus on elimination of the source of stress (Folkmann & Moskowwitz, 2004). In the case of the analyst, instead of taking a coffee break, the analyst might seek assistance from a more experienced colleague in order to mitigate the incident as quickly as possible and eliminate the source of stress. Beyond elimination of the stress source, problem-focused coping methods help facilitate adaptive responses to stress (Folkman & Moskowitz, 2004). More information on adaptability can be found in Chapter 7: "Collaborative Problem-Solving."

Early research indicated that problem-focused coping methods were more effective than emotion-focused methods (Keoske, Kirk, & Keoske, 1993). However, when sources of stress are not controllable, as might be the case in incident response, emotion-focused methods can prove beneficial. In the case of a CSIRT, a watch team member might not be able to exert control during an incident because he or she is not directly involved in examining forensics or making changes to the system under attack. In this scenario, taking a coffee break might prove more beneficial because it provides the CSIRT analyst with time to recover from the stress experienced during the incident, thereby providing the analyst with more energy if he or she needs to re-engage in the incident response process (Chapter 10 provides information on effectively implementing employee breaks).

CSIRT managers can encourage the use of effective coping methods among their CSIRT members in several ways. We refer readers to the Collaborative Problem-Solving chapter (Chapter 7). Additionally, Britt and Jex (2015) suggest that managers engage in activities that encourage their employees to adopt positive coping methods. A list of possible manager activities (adapted from Britt & Jex, 2015) is found in Table I.2.

People who work in stressful environments can greatly benefit from developing their individual resilience. Through such developments, they can maintain their individual performance, mental and physical well-being, and be an effective resource for others with whom they interact, such as teams and organizations of which they are members. However, well-developed individual resilience does not guarantee that the teams and organizations of which they are members will remain resilient to stress and adversity. The occurrence of stress can still negatively impact team processes and ultimately team performance and effectiveness. In the next section, we review team resilience in an effort to identify ways to maintain team processes.

I.4.3 COLLECTIVE (TEAM) RESILIENCE

Team resilience refers to "the capacity of a team to withstand and overcome stressors in a manner that enables sustained performance" (Alliger et al., 2015, p. 177). The collective actions of individual team members during stressful circumstances reflect how teams demonstrate resilience. By maintaining team processes during times of adversity, teams can appropriately manage new challenges, or at the very least, minimize potential negative consequences that arise when challenged (Zaccaro et al., 2011). Further, certain team characteristics (e.g., team structure, norms, and values) can serve as precursors to effective team processes (Mathieu, Maynard, Rapp, & Gilson, 2008). In this section, we review how teams maintain effective team processes and various team characteristics that can impact these processes.

TEAM PROCESSES

During times of stress and adversity, team processes can break down or be disrupted (Zaccaro et al., 2011). When these processes break down, teams can experience a variety of negative events. Cohen (1980) suggested that increased stress could result in information overload for individuals who must focus their attention on novel aspects (i.e., anomalies) associated with a task. Team members in these circumstances potentially become more focused on task specific needs, or possibly their own individual needs, rather than the needs of the team, which might require more effort (e.g., collaboration). As team members become more individualistic, teams tend to experience less effective decision-making, cohesion, coordination, and communication, which can eventually result in lowered team performance and effectiveness (Driskoll, Salas, & Johnston, 1999). Figure I.2 summarizes these aspects of team resilience.

Maintaining team processes under adversity.

A common assumption is that a collection of resilient individuals will result in a resilient team. However, as demonstrated by many chapters of this handbook, there are other influences on team

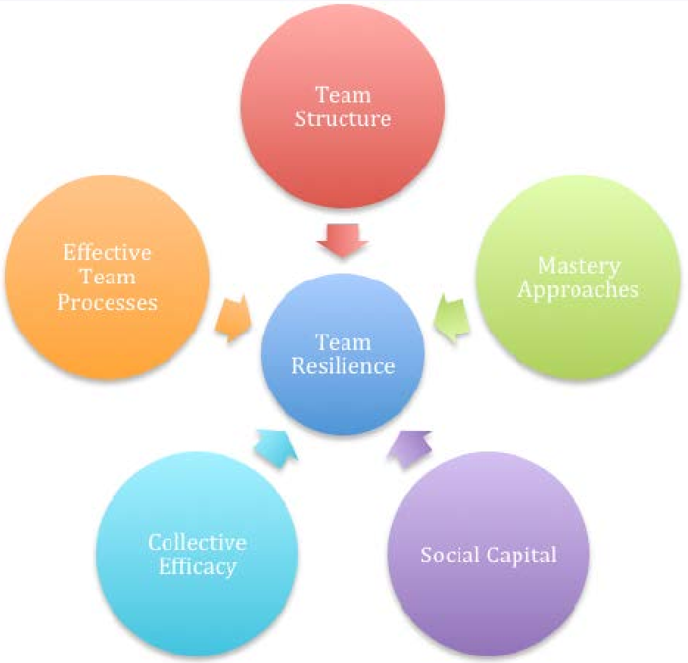


Figure I.2 Factors that Compose Collective (e.g., Team) Resilience.

processes. We refer readers to Chapters 5, 6, 7, 8, and 9 for additional information on maintaining team processes. One specific approach that aligns well with incident response stems from work by NASA that is used to help multiteam systems involved in space travel, a highly stressful environment where stressful incidents must be resolved correctly and quickly (Noe, Dachner, Saxton, Keeton, & EASI, 2011). During times of adversity and under high levels of stress, maintenance of effective team processes must occur so that individuals do not become too focused on their own reactions to the stress they experience. In order to maintain team processes, CSIRTs must be prepared for adversity, able to function during times of adversity, and, perhaps most importantly, be able to learn from adversity and improve team processes before additional stressful circumstances arise. Alliger, Cerasoli, Tannenbaum, & Vessey (2015, p. 187) referred to these three actions as “minimize,” “manage,” and “mend.”

Minimize. Resilient teams are proactive and attempt to address problems before they create any lasting damage. In other words, they minimize the potential for increased stress by anticipating and planning for various challenges. Through this process, resilient teams can avoid some problems and potentially reduce the damaging effects of unanticipated problems. According to Alliger et al. (2015, pp. 178-179) resilient CSIRTs can minimize stress associated with incident response in four ways: 1) “anticipate challenges and plan contingencies,” 2) “understand current readiness,” 3) “identify early warning signs of potential problems,” and 4) “prepare to handle difficult circumstances.” The Contingency Planning section in Chapter 7 describes strategies CSIRTs can use to anticipate and effectively overcome challenges.

Manage. Not all stressful circumstances can be predicted, as is often the case with incident response. Under such circumstances, adverse events must be effectively managed as they occur. According to Alliger et al. (2015, pp. 179-180) resilient teams can manage challenging circumstances in five ways: 1) they “assess challenges quickly, honestly, and accurately,” 2) they “address chronic stressors,” 3) they ”provide backup and assistance to one another,” 4) they “consciously maintain basic processes under stress,” and 5) they “seek guidance.” Additional improvement strategies listed in Chapter 7 can be implemented to help teams effectively manage adverse events by developing their ability to adapt, specifically when faced with novel or non-routine events.

Mend. Another important characteristic of resilient teams is their ability to recover from stressful experiences in ways that enable the team to learn from experience and adapt their behaviors. According to Alliger et al. (2015, p. 180) teams can mend the team functions that were affected by adversity in four ways: 1) they “regain situational awareness as quickly as possible,” 2) they “debrief,” 3) they “address concerns or risk points that became evident during the challenging encounter,” and 4) they “express appreciation.” We also refer readers to the improvement strategies for continuous learning listed in Chapter 11.

Similar to the way individual characteristics (e.g., personality) can serve as precursors to individual resilience, certain team characteristics also help “set the stage” for a team’s ability to maintain effective team processes. Some of these team characteristics are reviewed in the next section.

CHARACTERISTICS OF RESILIENT TEAMS

Teams are often described by various characteristics, such as their compositional structure or collective behaviors. Morgan et al. (2013) identified four characteristics that lead to the development of resilient teams: team structure, mastery approaches, social capital, and collective efficacy.

Team Structure. Various aspects surrounding how teams are structured impact how they function because they reflect physical aspects of the group as well as psychological aspects that can develop through the generation of team norms and values. Teams typically have a formal structure that reflects composition and resources (e.g., required experience and expertise, number of team members). Such structural aspects influence intra-team and between-team coordination based on team members' shared understandings of team processes (Malakis & Kontogiannis, 1997).

With regard to team structure, teams should ensure that they are composed of enough members to sufficiently cover all aspects of team operations, both during times of low and high stress. Further, team norms, such as a shared vision, a sense of purpose, or common goals can greatly influence team responses to stress because they provide guidance on how to act under specific circumstances. For example, if one analyst notices another analyst getting distracted by a specific part of the problem that is not related to a current goal, he or she can remind the other analyst of the goal and re-focus the analyst's behavior toward the goal at hand.

Mastery Approaches. Team members can develop similar attitudes as a result of shared common experiences. These common expectations about certain events can enable team members to be more adaptable to new experiences because the team does not have to waste time learning and understanding the situation. Similarly, teams that tend to focus on the development of individual team members, and the development of the team as a whole, often reflect a learning orientation that increases adaptability in the face of novel circumstances. When everyone shares an understanding about a specific incident, CSIRT members can filter out non-important cues that might distract them during the incident response process. By focusing on the important aspects of the situation, they can maintain focus and put their cognitive resources toward anticipating or adjusting to novel stressors. We refer readers to Chapter 11 for more information on learning and Chapters 1, 5 and 7 for information on adaptation.

Social Capital. Just as social support is important for individual resilience, social capital is important for team resilience. Social capital refers to the positive benefits for individuals and groups that stem from participation and involvement in teams (Aldrich & Meyer, 2015). These benefits can stem from a common group identity, perceptions of available social support, and pro-social interactions with others (Morgan et al., 2013) and can lead to improved collective (e.g., team) processes based on shared trust among individuals (Leana & Van Buren, 1999).

To improve the social capital of CSIRTs, managers can encourage team members to engage in team bonding activities (e.g., getting together for social, non-work related reasons). They can also encourage the development of a team identity by encouraging team members to engage in team building activities that enhance collaboration, mutual accountability, positive team cultures, strong communication processes, and trust among others. Research by Yukelson (2008) describes common approaches among athletic teams taken from research on organizational development and team dynamics that can be applied to CSIRTs.

Collective Efficacy. The concept of self-efficacy (mentioned above) can also be applied to group settings (i.e., teams). Teams can experience collective efficacy when they hold collective beliefs about what the team is capable of achieving (Bandura, 1982). Teams low in collective efficacy tend to be less satisfied with their work, particularly under high workloads, and are less committed to their organizations when the work they do is not perceived as significant (Jex & Bliese, 1999). High workloads and negative perceptions of work tasks increase stress experienced by employees. Individuals and teams who believe they can still succeed under such circumstances react less to these stressors and demonstrate greater resilience.

To increase the collective efficacy of teams, CSIRT managers can remind team members of their past successes to increase their confidence and belief that the team can be successful (although again, we caution against the notion of overconfidence described above) (Bandura, 1982). Shared successful experiences not only increase the knowledge and expertise of the group, but also impact group cohesion as well. When group cohesion is high, team members are supportive of one another and can feel as if they are "in the fight together". Further, teams that communicate and share feedback among team members after disappointment occurs tend to be more resilient and feel supported for future challenges (Morgan et al., 2013). We refer readers to Chapter 5 for information on team communication.

In the next section, we review specific programs designed to foster resilience among individuals and/or teams. We conclude with a review of the CSIRT leader's role in fostering resilience among his or her CSIRT members and teams and a summary of resources readers might find helpful.

I.4.4 HOW TO ENHANCE AND DEVELOP SOCIAL RESILIENCE

Several training programs have been developed to enhance individual and team resilience. Many of these are used primarily in VUCA environments (e.g., military and medical settings) and could, therefore, prove beneficial for CSIRTs as well. However; it is important to note that these training programs should be empirically validated to determine the extent to which they improve individual and collective resilience in CSIRTs. We highlight a few of them below.

Battlemind Training and the Comprehensive Soldier Fitness Program

"Battlemind" refers to a "soldier's inner strength to face fear and adversity in combat with courage" (Castro et al., 2006, p.1).

The U.S. Army developed Battlemind training based on research from the Walter Reed Army Institute of Research to help soldiers prepare for deployment and later extended it to help them reintegrate to home life after returning from combat (Castro et al., 2006). Examples used in the program focus on topics such as unit cohesion, support from peers and leaders for those who experience difficulty in making the transition to non-combat life, safety (e.g., behaviors that help in combat might be inappropriate at home), relationships, and dealing with the prolonged or delayed-onset of physical, social, and psychological reactions to combat. Throughout training, a cognitive skills-based approach helps soldiers reframe stressful situations and reinforce adaptive ways of thinking. For example, anger and hypervigilance are common reactions after soldiers are involved in combat. Battlemind training helps soldiers view these reactions not as problems, but as natural consequences of work-related coping skills developed for combat (Castro et al., 2004). In other words, a soldiers' survival during combat depended on his or her ability to make split-second decisions while being alert and aware. At home, however, soldiers might overreact to minor events or feel anxious in large groups where it is difficult to evaluate everything. Through Battlemind training, soldiers can learn to recognize that at home it is more appropriate to think and take time to relax instead of reacting. Many combat skills are focused on throughout the training and sessions also include debunking stigmas often associated with seeking mental health assistance.

Soldiers who go through Battlemind training are educated on "6 Tough Facts about Combat" that include (Castro et al., 2006, p. 3):

- "Combat is difficult."
- "The combat environment is harsh and demanding."
- "Fear in combat is not a weakness."
- "Soldiers are afraid to admit that they have a mental health problem."
- "Deployments place a tremendous strain upon families."
- "Unit cohesion and team stability are disrupted by combat" (Castro et al., 2006, p. 3)."

CSIRT leaders could adapt aspects of Battlemind training in an effort to help team members reframe stress experienced on the job and identify adaptive ways of thinking about that stress. For example, teams could create their own "Tough Facts" about incident response, such as "The incident response process is stressful and demanding" and "Team processes can be disrupted by complex incidents". Once this list is created, teams could brainstorm ideas for managing the stress associated with each "tough fact" or attempt to brainstorm creative ways to lessen the potential stress that might arise during high stress incidents.

Hardiness Training

Several training methods exist that aim to increase individuals' ability to demonstrate hardiness. Programs such as the HardiTraining Program developed by Maddi (1987; 2013) and The Hardiness Training Program (HTP; Judkins et al., 2006) based on the Maddi (1987; 2013) and others (e.g., Rowe, 1999), focus on a range of topics related to personal resilience and stress management. HardiTraining (Maddi, 1987, 2013) contains on three components that contribute to hardiness and resilience. The first is situational reconstruction, which entails re-imagining stressful situations in ways that increase the possibility of more positive outcomes. The second is focusing, which fosters sense-making and the re-framing of stressful situations. The third component is compensatory self-improvement, which involves placing greater emphasis on stressful situations that are more controllable. The exercises in these components focus on problem solving, coping, building supportive relationships, and engaging in self-care.

HardiTraining and HTP have been used to help students (Maddi, 1987; Maddi et al., 2002; Maddi et al., 2009) and employees (e.g., nursing managers; Judkins et al., 2006) effectively cope with the demands they face and reduce frustration, burnout, and turnover. Information on the original hardiness training program developed by Maddi (1987) is available at the following website: http://www.hardinessinstitute.com/?page_id=1197. The Hardiness Institute has a Train-the-Trainer program that certifies facilitators to work in organizational settings.

Stress Management and Resiliency Training (SMART)

The Stress Management and Resiliency Training (SMART) Program aims to increase resilience and quality of life for individuals while decreasing stress and anxiety (Sood et al. 2011). In this program, participants are instructed on meditation and breathing techniques that promote relaxation and reduce felt stress. They also receive follow-up sessions on an as-needed basis. Sood et al. (2011) found that participants experienced improvement in several markers of resilience. Information on this program can be found at http://www.stressfree.org/programs/smart.

Additional Ways Leaders Can Enhance the Social Resilience of CSIRTs

CSIRT leaders can enhance the social resilience of their CSIRTs by influencing how individuals and teams engage in and react to stress associated with incident response. Ensuring their teams maintain basic functions during stressful incident response scenarios could help team processes continue to function effectively. Many ways to influence positive team processes are described throughout this handbook and are summarized here to reflect their potential impact on social resilience. For instance, CSIRT leaders could enhance team processes by having clearly documented tools and standard operating procedures for their teams. To the extent that certain types of incidents, or specific incident characteristics, can be anticipated, checklists or guidebooks can be useful to ensure basic actions are completed and role expectations are clear. Such tools could be helpful during unexpected circumstances when it might be important to maintain basic processes. For example, incident response teams could be provided with step-by-step procedures that outline escalation guidelines, key questions to ask, or other trouble-shooting tips that might prove helpful when teams are faced with unexpected high workloads.

CSIRT managers could also make sure that their teams maintain written, up-to-date standardized operating procedures and reference books (e.g., contact lists of key resources). These resources would help CSIRTs maintain basic operations during stressful times when it can be easy to forget about simple or basic team actions, or when back-up actions might be warranted between co-workers. Another benefit of these tools is that they free up people's mental capacity to deal with more challenging, complex work. Additional information on the development of checklists and guidebooks can be found in Chapters 5 and 7.

CSIRT managers could also work with their team members to determine warning signs of stressful circumstances. These discussions could be held during "Lessons Learned" discussions associated with stressful incidents to help team members become aware of situations where team processes might break down or become less effective. Teams can then increase their resilience by developing action plans for coping with similar circumstances in the future. We refer readers to Chapter 11 for information on conducting effective After-Action Reviews.

In Table I.3, we provide a variety of other resources that might prove useful for CSIRT leaders seeking to develop social resilience within their CSIRT. These resources cover a variety of tools including additional resilience programs, assessment tools, and useful sources that provide information on individual and team behaviors and characteristics linked with resilience.

I.5 Conclusion

The incident response process often requires continuous learning and adaptation to be effective. Individuals' and teams' abilities to demonstrate resilience can greatly influence the extent to which CSIRTs learn from and adapt to stressful circumstances. In doing so, CSIRTs can complement technological resilience, which is often the focus in incident response, with enhanced social resilience. We described the characteristics and behaviors associated with social resilience among individuals and teams. CSIRTs that demonstrate resilience when challenged with stressful circumstances set the foundation for future development that, if done right, will continue to enhance the teams' effectiveness in mitigating complex cyber-attacks.

TABLE I.3 RESOURCES TO HELP DEVELOP INDIVIDUAL AND TEAM RESILIENCE

RESOURCE	DESCRIPTION	WHERE TO FIND
ASSESSMENT TOOLS*		
The Brief Resilience Scale	Measures recovery ability	Smith et al. (2008)
Psychological Resilience	Assesses the protective factors of self-esteem, personal competence, and interpersonal control	Windle et al. (2008)
The Resilience Scale	Personality-based measurement (assesses personal competence and acceptance of self and life)	Wagnild & Young (1993) http://www.resiliencescale.com/wp-content/uploads/2014/06/Wagnild-Young-psychom-R.pdf
Ashridge Resilience Questionnaire (ARQ)	Designed for managers to assess their personal resilience.	https://www.ashridge.org.uk/executive-organization-development/psychometrics/other-ashridge-instruments/
The Dispositional Resilience Scale	Measurement of hardiness	http://www.hardiness-resilience.com/docs/AP-S95HAN1.pdf
Resilience	Measurement based on the Five-Factor Model of personality as related to components of resilience	http://www.robertsoncooper.com/iresilience/
Mental Toughness Questionnaire (fee required)	Assesses the ability to withstand pressure	http://www.aqr.co.uk/page/mtq48

*These tools are not meant for formal assessment.

TABLE I.3 RESOURCES TO HELP DEVELOP INDIVIDUAL AND TEAM RESILIENCE (CONT.)

RESOURCE	DESCRIPTION	WHERE TO FIND
ASSESSMENT TOOLS*		
RESILIENCE PROGRAMS		
HardiTraining	A program designed to develop hardiness among individuals	http://www.hardinessinstitute.com/
Battlemind	U.S. Army program focused on pre-deployment and transition development	Adler et al. (2009)
Comprehensive Soldier & Family Fitness Program	"Designed to increase psychological strength and positive performance, and to reduce the incidence of maladaptive responses of the entire U.S.Army" (Cornum, Matthews, Seligman, 2011, p. 4)	http://www.acsim.army.mil/readyarmy/ra_csf.htm
Master Resiliency Training	U. S. Army program aimed at developing emotional, social, spiritual, family, and physical strengths	Griffith & West (2013)
Mental Toughness Training	Various resources including training programs and keynote speakers	https://mentaltraininginc.com/
University of Pennsylvania Resilience Training Program	Program focusing on the prevention and reduction of stress-related problems	http://ppc.sas.upenn.edu/services/penn-resilience-training
R.E.A.D.Y Program	REsilience and Activity for every DaY Program for team resilience	Burton et al. (2010)
S.M.A.R.T. Program	Stress Management and Resilience Training Program (reviewed above)	http://www.stressfree.org/programs/smart
S.T.R.I.V.E.	Stress Resilience In Virtual Environments – focuses on coping skills and stress assessment	http://ict.usc.edu/prototypes/strive/
STRESS TRAINING		
Digital Game Training for Burnout	Article on the use of a digital online game based on cognitive-behavioral therapy for burnout treatment.	Zielhorst et al. (2015)
Worksite Stress Management Training	Stress management training based on acceptance and commitment therapy.	Flaxman & Bond (2010).
Useful Publications (Title or Topic)		
Building resilience for success:A resource for managers and organizations	Book	Cooper, Flint-Taylor, & Pearn (2013)
Hardiness: Turning stressful circumstances into resilient growth	Book	Maddi (2013)
The resilience factor	Book	Reivich & Shatté (2002)
Thriving under stress: Harnessing demands in the workplace	Book	Britt & Jex (2015)
List of breaks and their impact	Article	Fritz, Lam, & Spreitzer (2011)
Summary of stress training skills	Article	Driskell, Johnston, & Salas (2001)

***These tools are not meant for formal assessment.**

References

Adler, T., Black, J.A., & Loveland, J.P. (2003). Complex systems: Boundary-spanning training techniques. *Journal of European Industrial Training, 27*(2-4), 111-124.

Aldrich, D. P., & Meyer, M. A. (2015). Social capital and community resilience. *American Behavioral Scientist, 59*(2), 254-269.

Alliger, G. M., Cerasoli, C. P., Tannenbaum, S. I., & Vessey, W. B. (2015). Team resilience: How teams flourish under pressure. *Organizational Dynamics, 44*(3), 176-184.

Bandura, A. (1982). Self-efficacy mechanisms in human agency. *American Psychologist, 37*, 122-147.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. New York: Freeman.

Beehr. T. A. (1995). *Psychological Stress in the Workplace.* London: Routledge.

Britt, T. W., & Jex, S. M. (2015). *Thriving under stress: Harnessing demands in the workplace*. Oxford University Press, USA.

Burton, N. W., Pakenham, K. I., & Brown, W. J. (2010). Feasibility and effectiveness of psychosocial resilience training: A pilot study of the READY program. *Psychology, Health & Medicine, 15*(3), 266-277.

Cacioppo, J. T., Adler, A. B., Lester, P. B., McGurk, D., Thomas, J. L., Chen, H. Y., & Cacioppo, S. (2015). Building social resilience in soldiers: A double dissociative randomized controlled study. *Journal of Personality and Social Psychology, 109*(1), 90.

Cacioppo, J. T., Reis, H. T., & Zautra, A. J. (2011). Social resilience: The value of social fitness with an application to the military. *American Psychologist, 66*(1), 43.

Castro, C. A., Hoge, C. W., & Cox, A. L. (2006). *Battlemind training: Building soldier resiliency*. Walter Reed Army Institute Of Research, Silver Spring, MD. Deptartment of Military Psychiatry.

Cohen, S. (1980). Aftereffects of stress on human performance and social behavior: A review of research and theory. *Psychological Bulletin, 88*(1), 82.

Connor, K. M., & Davidson, J. R. (2003). Development of a new resilience scale: The Connor-Davidson Resilience Scale (CD-RISC). *Depression and Anxiety, 18*(2), 76-82.

Connor-Smith, J. K. & Flachsbart, C. (2007). Relations between personality and coping: A meta-analysis. *Journal of Personality and Social Psychology, 93*(6), 1080-1107.

Cornum, R., Matthews, M. D., Seligman, M. E. P. (2011). Comprehensive, soldier, fitness: Building resilience in a challenging context. *American Psychologist, 66*, 4-9.

De Lange, A. H., Taris, T. W., Kompier, M. A., Houtman, I. L., & Bongers, P. M. (2004). The relationships between work characteristics and mental health: Examining normal, reversed and reciprocal relationships in a 4-wave study. *Work & Stress, 18*(2), 149-166.

Folkman, S., & Moskowitz, J. T. (2004). Coping: Pitfalls and promise. *Annual Review of Psychology, 55*, 745-774.

Friborg, O., Hjemdal, O., Rosenvinge, J. H., & Martinussen, M. (2003). A new rating scale for adult resilience: What are the central protective resources behind healthy adjustment? *International Journal of Methods in Psychiatric Research, 12*(2), 65-76.

Friborg, O., Barlaug, D., Martinussen, M., Rosenvinge, J. H., & Hjemdal, O. (2005). Resilience in relation to personality and intelligence. *International Journal of Methods in Psychiatric Research, 14*(1), 29-42.

Garmezy, N., Masten, A. S., & Tellegen, A. (1984). The study of stress and competence in children: A building block for developmental psychopathology. *Chile Development, 55*, 97-111.

Griffith, J., & West, C. (2013). Master resilience training and its relationship to individual well-being and stress buffering among Army National Guard soldiers. *The Journal of Behavioral Health Services & Research, 40*(2), 140-155.

Hardy, G. E., Woods, D., & Wall, T. D. (2003). The impact of psychological distress on absence from work. *Journal of Applied Psychology, 88*(2), 306.

Heath, C., Larrick, R. P., & Klayman, J. (1998). Cognitive repairs: How organizational practices can compensate for individual shortcomings. In Review of Organizational Behavior.

Hobfoll, S. E. (2001). The influence of culture, community, and the nested-self in the stress process: Advancing conservation of resources theory. Applied Psychology: An International Review, 50, 337–421.

Hobfoll, S. E., & Lilly, R. S. (1993). Resource conservation as a strategy for community psychology. *Journal of Community Psychology, 21*, 128–148.

Jex, S. M., & Bliese, P. D. (1999). Efficacy beliefs as a moderator of the impact of work-related stressors: A multilevel study. *Journal of Applied Psychology, 84*(3), 349.

Judkins, S., Reid, B., & Furlow, L. (2006). Hardiness training among nurse managers: Building a healthy workplace. *The Journal of Continuing Education in Nursing, 37*(5), 202-207.

Kaspersky Lab (2013). Big stakes for small business security – Can your business afford and IT security incident? Retrieved from http://www.kaspersky.com/about/news/business/2013/Big_Stakes_for_Small_Business_Security_Can_your_Business_Afford_an_IT_Security_Incident

Keizer, G. (2011, Sept. 21). Retrieved from: http://www.computerworld.com/article/2511297/security0/diginotar-dies-from-certificate-hack-caper.html

Keoske, G. F., Kirk, S. A., & Keoske, R. D. (1993). Coping with job stress: Which strategies work best? *Journal of Occupational and Organizational Psychology, 66*, 319-355.

Kinicki, A. J., & Latack, J. C. (1990). Explication of the construct of coping with involuntary job loss. *Journal of Vocational Behavior, 36*(3), 339-360.

Kobasa, S. C. (1979). Stressful life events, personality, and health: An inquiry into hardiness. *Journal of Personality and Social Psychology, 37*(1), 1.

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. New York, NY: Springer publishing company.

Leana, C. R., & Van Buren, H. J. (1999). Organizational social capital and employment practices. *Academy of Management Review, 24(*3), 528-555.

Liossis, P. L., Shochet, I. M., Millear, P. M., & Biggs, H. (2009). The Promoting Adult Resilience (PAR) program: The effectiveness of the second, shorter pilot of a workplace prevention program. *Behaviour Change, 26*(02), 97-112.

Maddi, S. R. (1987). Hardiness training at Illinois bell telephone. *Health Promotion Evaluation*, 101-115.

Maddi, S. R. (1999). The personality construct of hardiness: I. Effects on experiencing, coping, and strain. *Consulting Psychology Journal: Practice and Research, 51*(2), 83.

Maddi, S. R. (2002). The story of hardiness: Twenty years of theorizing, research, and practice. *Consulting Psychology Journal: Practice and Research, 54*(3), 173.

Maddi, S. R. (2004). Hardiness: An operationalization of existential courage. *Journal of Humanistic Psychology, 44*(3), 279-298.

Maddi, S. R. (2012). *Hardiness: Turning stressful circumstances into resilient growth*. Springer Science & Business Media.

Maddi, S. R., & Kobasa, S. C. (1984). *Hardy executive*. Dow Jones-Irwin.

Magnavita, Jeffrey J. (2004) *Handbook of personality disorders: theory and practice* John Wiley and Sons.

Malakis, S., & Kontogiannis, T. (2008, October). Cognitive strategies in emergency and abnormal situations training: implications for resilience in air traffic control. In *Proceedings of the 3rd Symposium on Resilience Engineering*.

Maslach, C., Schaufeli, W. B., & Leiter, M. P. (2001). Job burnout. *Annual Review of Psychology, 52*(1), 397-422.

Mathieu, J., Maynard, M. T., Rapp, T., & Gilson, L. (2008). Team effectiveness 1997-2007: A review of recent advancements and a glimpse into the future. *Journal of management, 34*(3), 410-476.

Morgan, P. B., Fletcher, D., & Sarkar, M. (2013). Defining and characterizing team resilience in elite sport. *Psychology of Sport and Exercise, 14*(4), 549-559.

Noe, R. A., Dachner, A. M., Saxton, B., Keeton, K. E., & EASI, N. (2011). *Team training for long-duration missions in isolated and confined environments: A literature review, an operational assessment, and recommendations for practice and research*. NASA Report TM-2011-216612.

Richardson, G.E., Neiger, B., Jensen, S., & Kumpfer, K. (1990). The resiliency model. *Health Education, 21*, 33–39.

Rowe, M. (1999). Teaching health-care providers coping: Results of a two-year study. *Journal of Behavioral Medicine, 22*(5), 511-527.

Russo, J. E., & Schoemaker, P. J. (1992). Managing overconfidence. *Sloan Management Review, 33*(2), 7.

Schaufeli, W. B., & Bakker, A. B. (2004). Job demands, job resources, and their relationship with burnout and engagement: A multi-sample study. *Journal of Organizational Behavior, 25*(3), 293-315.

Smith, B. W., Dalen, J., Wiggins, K., Tooley, E., Christopher, P., & Bernard, J. (2008). The brief resilience scale: Assessing the ability to bounce back. *International Journal of Behavioral Medicine, 15*(3), 194-200.

Sood, A., Prasad, K., Schroeder, D., & Varkey, P. (2011). Stress management and resilience training among Department of Medicine faculty: A pilot randomized clinical trial. *Journal of General Internal Medicine, 26*(8), 858-861.

Stiehm, J. H. (2010). *US Army War College: Military education in a democracy*. Temple University Press.

The high cost of a security breach. (2013, Jun. 25). Retrieved from: http://www.computerworld.com/article/2511297/security0/diginotar-dies-from-certificate-hack-caper.html

Warr, (2007). Work, happiness and unhapiness. Mahwah, NJ: Erlbaum.

Windle, G., Markland, D. A., & Woods, R. T. (2008). Examination of a theoretical model of psychological resilience in older age. *Aging and Mental Health, 12*(3), 285-292.

Yukelson, D. (1997). Principles of effective team building interventions in sport: A direct services approach at Penn State University. *Journal of Applied Sport Psychology, 9*(1), 73-96

Zaccaro, S. J., Weiss, E. J., Hilton, R. M., & Jeffries, J. (2011). Building resilient teams. *Leadership in dangerous contexts: A handbook for the armed forces, emergency services, and first responders*, 182-201.

Zielhorst, T., van den Brule, D., Visch, V., Melles, M., van Tienhoven, S., Sinkbaek, H., ... & Lange, A. (2015). Using a digital game for training desirable behavior in cognitive–behavioral therapy of burnout syndrome: A controlled study. *Cyberpsychology, Behavior, and Social Networking, 18*(2), 101-111.