CSIRT Information Sharing Workshop

Shari L. Pfleeger, Ph.D.
Lois E. Tetrick, Ph.D.
Reeshad S. Dalal, Ph.D.
Stephen J. Zaccaro, Ph.D.
Julie A. Steinke, Ph.D.

Amber Hargrove, M.A.
Daniel Shore, M.A.
Kristin M. Repchick, M.A.
Laura Fletcher, B. A.
Project Information

Project funded by:
• The U.S. Department of Homeland Security, Science & Technology Directorate (BAA 11-02)
• Dutch National Cyber Security Centre
• Swedish Civil Contingencies Agency

Full Research Team:
Examining CSIRT Effectiveness

CSIRTs can benefit from both technical and non-technical evaluations of effectiveness.

**NEEDS**
- Majority of current research focused on technological aspects; team interactions should be considered

**APPROACH**
- Applied behavioral science approach
  - Individual, team, and multiteam system (MTS) levels of CSIRT functions

**BENEFITS**
- Added layer of insight that is customizable and flexible around specific CSIRT needs
  - Provides a competitive advantage by integrating technical and non-technical guidelines and evaluations

**COMPETITION**
Project Overview

1. Data Collection
   - Collect data from individual interviews with CSIRT managers, focus groups with team members, and survey instruments

2. Identifying Knowledge, Skills, and Abilities

   - Team Staffing
   - Selection Systems
   - Training
   - Decision Aids
Presentation Roadmap

DATA
PROCESS
PROPOSITIONS
MTS
CTA
HANDBOOK
DISCUSSION
## Data: Focus Groups

<table>
<thead>
<tr>
<th>Total Interviewees</th>
<th>CSIRT Teams (focus group total)</th>
<th>Leader Interviews</th>
<th>MTS Leader Interviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>130+*</td>
<td>48**</td>
<td>19</td>
<td>10</td>
</tr>
</tbody>
</table>

### CSIRT Types

<table>
<thead>
<tr>
<th>Coordinating</th>
<th>Managed Service (external clients)</th>
<th>Corporate (internal)</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>10</td>
<td>16</td>
<td>6</td>
</tr>
</tbody>
</table>

*FG participants anonymous – total interviewees estimated from transcript review where not directly noted.**

**Among the largest number of CSIRT interviews conducted in a single CSIRT research project.
Data: KSAO Survey

- Survey of Knowledge, Skills, Abilities, and Other important attributes (KSAOs)
- Leader interviews and focus groups endorsed 46 attributes
- Survey designed to verify those observations
- Surveyed over 80 CSIRT professionals
  - National and corporate CSIRTs

Identified “Top 20” KSAOs
Endorsed as “very important”
TOP 20 CSIRT KSAOs

Cognitive
- Learning ability
- Problem-solving skills
- Investigative skills
- Intelligence
- Decision-making Competence

Character
- Work Ethic
- Specific Curiosity
- Resilience
- Self-motivated
- Detail-oriented
- Proactive
- Adaptive
- Perseverance
- Diverse Curiosity
- Ambiguity Tolerance

Social/Team
- Trustworthiness
- Collaborative problem-solving
- Motivation to work on behalf of team
- Communication skills
- Mentor/coaching ability
Effective CSIRT Performance

• CSIRT performance requires:

  **Taskwork:**
  • Detect and respond to incidents
  • Triage incoming incidents
  • Analyze incidents
  • Develop and execute comprehensive solutions

  **Teamwork:**
  • Solve problems collectively
  • Assess team performance
  • Give, seek, and receive task-clarifying feedback
  • Active listening skills
  • Knowledge about team members’ roles
Effective CSIRT Performance

• Behavioral science research
  • Helps explain how and why CSIRTs can be more effective

• Three-level CSIRT Framework
  - Individual
  - Within Team (Component Team)
  - Between Team (Multi-Team System)
Research Observation Themes

- Performance
- Cyber Security Work
- Individual Capacities
- Contextual Influences
Key Research Observations

• CSIRT/CERT work:
  • Occurs in complex and quickly changing environments
  • Requires effectively managing information and knowledge in a data rich context
  • Depends upon collaboration among individuals and teams
Key Research Observations

CSIRTs are multilevel

“Yeah. And so there's sort of different levels of success. There's one for your team and you as an individual as well. But then success also gets the other people on board and for them to do what they need to do to fix the issue.”

“You’re not only communicating between teams; you’re communicating with a lot of other people. So, you basically need to know some of the technical terms . . . you will definitely need to know what’s being talked about.”

~CSIRT Focus Group Members
Key Research Observations

CSIRT work fundamentally involves:
• Information management
• Collaboration (arises through individual initiative)

“There [are] a lot of times where we just like do on the fly meetings where we discuss problems and share ideas and try to find solutions to problems. So … if somebody gets stuck we usually have a meeting like that and talk about it.”

“Well, if I don't feel comfortable like saying yes, this is an incident or no, it is not, I'll literally turn around. I mean, like guys, do you mind looking at this, and giving your input?”

~CSIRT Focus Group Members
Key Research Observations: Data Findings

- Collaborative problem-solving
  - Ranked in Top 10 KSAOs by CSIRT professionals
  - #3 KSAO in focus groups and interviews
Key Research Observations

Information sharing: Critical for success

“Basically communications is definitely important, because we work, like we explained, with each other and the other teams and other resources. So often, you've got to be able to communicate. I think that's very important.”

~CSIRT Focus Group Member
Key Research Observations: Data Findings

• Strong drive to learn and **share information** and skill in talking to others ranked #1 and #2 in focus groups and interviews

• Communication skills, collaborative problem-solving, and motivation to work on behalf of the team all ranked in the Top 20 KSAs by CSIRT professionals
Key Research Observations

Characteristics of effective CSIRT members:
• Attention to detail
• Curiosity
• Adaptable

“Attention to detail is important with any technical type job . . . correlating events.”

“You’ve got to kind of like to tinker with stuff. I think curiosity is the biggest thing.”

“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.”

~CSIRT Focus Group Members
Key Research Observations: Data Findings

- **Adaptability**
  - Ranked among **Top 15** KSAO by CSIRT professionals
  - **Top 5** KSAO in focus groups and interviews

- **Collaborative problem-solving**
  - Ranked in **Top 10** KSAOs by CSIRT professionals
  - **#3** KSAO in focus groups and interviews

- **Types of Curiosity**
  - Ranked in **Top 20** KSAO by CSIRT professionals (#3 and #19)
  - **#1** Top KSAO in focus groups/interviews

So what does this mean?
Research Implications & Strategies

Adaptability

• Adaptive first line analysts can enable teams to perform better
• Increasing team knowledge can enhance the adaptive capacity of teams.
  • Focus of team knowledge: Team tasks, team interactions, and task contingencies
• Adaptive thinking training (e.g., frame switching)

Strategies to Enhance Adaptability

• Adaptive thinking training (e.g., frame-switching)
• Cross-training
• Virtual documentation of task procedures and contingencies
Research Implications & Strategies

Collaborative Problem-Solving

- Team managers should identify when teamwork and collaboration becomes more necessary
  - Develop team interaction norms and expectations accordingly
- Training and hiring strategies should target within- and between-team collaboration.
- Consider “countervailing forces” that can arise among teams, and between teams and the MTS
Research Implications & Strategies

Strategies to Enhance Collaboration

• **Counterfactual thinking** (thinking about what “might have been”)
  • Can increase the amount of unshared or unique information shared among team members and improve decision-making accuracy (Galinsky & Cray, 2004).

• **Devil’s Advocacy** procedure: each team member advocates for a specific course of action
  • Can reduce premature decision-making
Research Implications & Strategies

Curiosity
• Includes seeking information, knowledge acquisition, learning, and thinking
• Some positions might involve higher levels of seeking ambiguous information than others

Strategies to Enhance Curiosity
• Hire highly curious individuals
• Train individuals to develop information-seeking skills
CSIRTs as Multiteam Systems

• Creating the best CSIRT is not enough

• CSIRTs typically operate as part of multiteam systems
CSIRTs as Multiteam Systems

• What are Multiteam Systems?
  • Teams interact interdependently
  • Teams share a common goal
    • Maintain separate team goals
  • Members’ functions and expertise
    • Similar within team
    • Different across teams
  • Dispersed teams
    • Geographically
    • Temporally
MTS Example: Emergency Medical Teams

EMT / Fire

Surgical

Recovery

Ambulance/Transport

Save Lives

Slides from Leslie DeChurch (used with permission)
MTS Example:
Port of Rotterdam

Adapted from: Uitdewilligen & Waller (2012)
CSIRTs as Multiteam Systems

Steady State MTS

Development

• Step 1 – I/O Psychologists
  • Reviewed data from 14 CSIRTs
  • Created team task statements and generic MTS structure diagrams for each CSIRT

• Step 2 – Subject Matter Experts
  • Independently verified and validated MTS structure
  • Edited structures accordingly

• Step 3
  • Verification with data collected from 6 additional CSIRTs
CSIR MTS Steady State Structure
CSIRTs as Multiteam Systems

• Remaining Questions
  • Is the steady state structure an accurate baseline depiction?
  • What changes the structure?
    • Incident severity
    • CSIRT maturity
  • What information is missing from the structure?
Cognitive Task Analyses

• A type of job analysis
  • Primarily for cognitive jobs
  • Identifies:
    • Thought processes
    • Decision-making skills

• Includes a variety of interview techniques
  • Explain process diagrams of decision-making steps
  • Discuss decisions made in challenging situations
  • Respond to hypothetical scenarios
Cognitive Task Analyses

• Hypothetical scenario
  • Frontline analyst in a small shop
  • Abnormally high network traffic
  • Outbound traffic going to a “.ru” domain

• Questions
  • What do you think is happening?
  • How confident are you that you know what’s happening?
  • How would you respond?
Cognitive Task Analyses

• People tend to be overconfident
• Overconfidence leads to:
  • Decreased adaptability
  • Increased errors
Cognitive Task Analyses

• Pre-Mortem Exercise
  • Prescriptive hindsight: Anticipatory thinking
    • How could someone fail?

• Preliminary Results
  • Decreased confidence (often too high)
  • Increases accuracy

• Applications
  • Prompts (e.g., Pop-up box during incidents)
  • Training exercises
Handbook on CSIRT Effectiveness

Table of Contents
1. Introductory Chapter
   • Intended Audience, How to use this book, etc.
2. CSIRTs in Their Operating Environment
3. Performance
4. Collective Problem Solving in Teams
5. Communication Skills
6. Successful Adaptation
7. Fostering a Learning Climate Among CSIRTs
8. Maintained Attention and Focus Over Time (Vigilance)
9. Maintained CSIRT Performance Under Adversity (Resilience)
10. Future Considerations/Where do we go from here
11. Appendices (e.g., white papers, taxonomy, assessment questions, developmental strategies)
Future Work

• Handbook Development
• Training Sessions Development
  • Expanded workshop
• Workshop Webinar
  • July 14
Discussion and Feedback

Questions or Comments:
Lois Tetrick, Ph.D.
ltetrick@gmu.edu