Cybersecurity Capacity Building

Brittany Manley

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

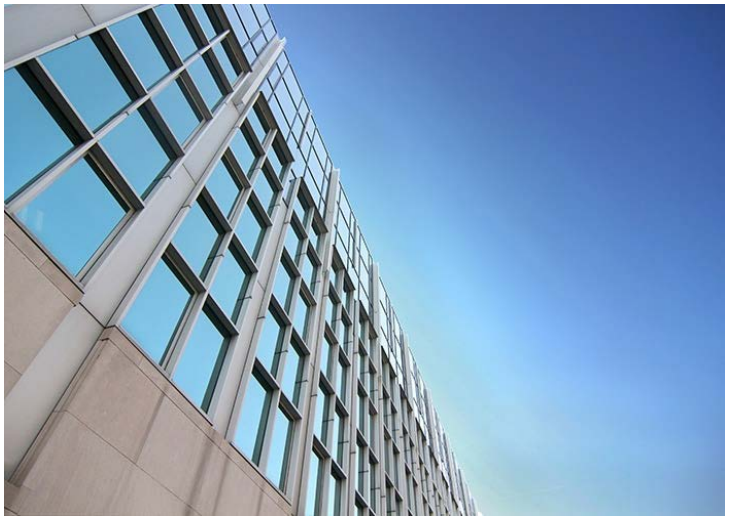
Notices

This material is based upon work funded and supported by the Department of State under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM20-0851

The Software Engineering Institute and the CERT Division

The Software Engineering Institute (SEI) at Carnegie Mellon University is a Federally Funded Research and Development Center (FFRDC)—a nonprofit, public–private partnership that conducts research for the United States government.



- **CERT** is the SEI's Cybersecurity Division, working to research security vulnerabilities in software products, contribute to long-term changes in networked systems, and develop cutting-edge information and training to improve the practice of cybersecurity.
- We provide partner agencies with expertise in a wide range of Cybersecurity fields including Cyber Intelligence, Cyber Workforce Development, Risk Management, Insider Threat, Security Operations, and more.

What We Do

CERT helps security operations and cybersecurity centers develop, operationalize, and improve their incident management capabilities to prevent and mitigate cybersecurity threats (“capacity building”).

- We support the U.S. Vision for Cyberspace and Approach to Cyberspace Policy through the following activities:
  - implementing and improving sustainable incident response capabilities with teams around the world
  - enhancing state-of-the-art techniques and practices in the cyber threat information-sharing field and applying this knowledge in a regional setting to promote trust-based incident response communities
  - developing the global cybersecurity workforce through tailored capacity building and mentoring

Cybersecurity & Incident Response

Cybersecurity threats pose significant risks to all organizations throughout the world and when computer security incidents occur, organizations must respond quickly and effectively.

You cannot completely prevent computer security incidents. Therefore, organizations must:

- Mitigate the risks.
- Be prepared to act when they do occur .

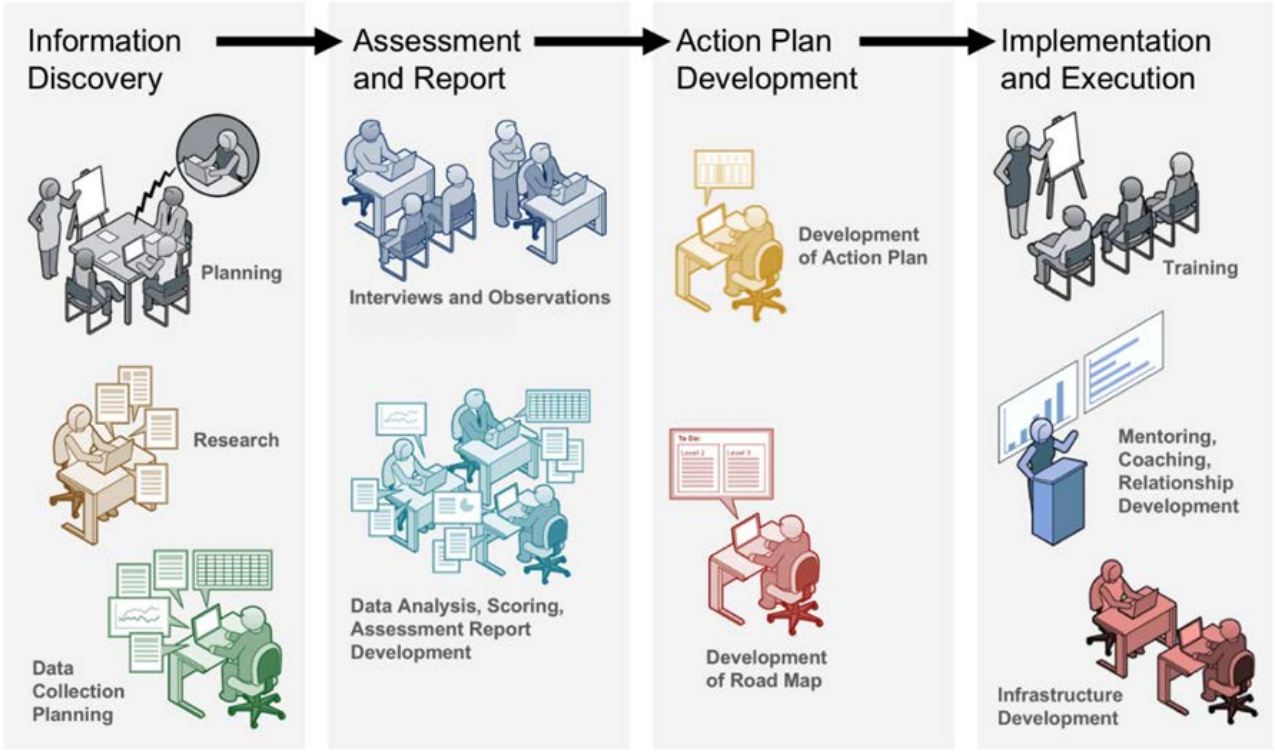
It is critical that an organization responds to cyber events quickly and effectively by recognizing, analyzing, and responding to incidents, thereby limiting damage and reducing recovery costs.

Cybersecurity Centers & Incident Response Teams

- Cybersecurity centers are essential to these incident response efforts.
- These centers may take the form of cybersecurity centers, computer security incident response teams (CSIRTs), security operations centers (SOCs), product security incident response teams (PSIRTs), or other similar incident management teams.
- The SEI helps prepare these cybersecurity center teams to effectively assess and manage cybersecurity incidents.

Given the increasing complexity and interdependence of the global information infrastructure, sustainable and successful national CSIRTs are an essential element to the overall cybersecurity of both a nation or economy and the global community.

Our Process



Cybersecurity Capacity Building

Threats & Challenges

Threat Environment

There is a growing **dependence** on the internet, along with a growing **interdependence** on technologies and interconnectedness.

- Legal/regulatory issues
  - compliance with data protection, privacy, and accountability (e.g., incident response) laws and liabilities
- All the while, hackers continue to advance, increasing the need for organizational precautionary measures.

Impact

- Data breaches
- Financial losses
- Loss of reputation/business
- Threats to human life/safety
- Compromise of national security

Threat Actors

- Professional cybercriminals
- Nation-state actors
- Hacktivists
- Insider threats

Threat Vectors

- Social engineering
- Exploitable vulnerabilities
- Insider threats
- Malware

Prevention and Protection

It is important to know the ways to prevent these methods and also how to counteract them.

- Do not open suspicious/untrusted emails, links, or attachments.
- Use two-factor authentication for passwords and make passwords different for each account.
- Backup files to an external hard drive.
- Keep your software updated.

Capacity Building supports methods of prevention and protection.

- Managed detection and response, monitoring and alerting
- Cyber threat intelligence
- Compliance reporting
- Addressing the steps of the cyber kill chain
- Frequent vulnerability scans
- Advisory services and audits
- Training and awareness activities

Common Challenges

Lack of

- Cybersecurity legislation, policy, or strategy
- Foundational organizational requirements – such as authority, mandate, mission, etc.
- Clear roles and responsibilities
- Sufficient funding and resources
- Leadership support
- Trust among constituents
- Information sharing
- Trained staff

Cybersecurity Capacity Building

SEI/Georgia Activities

SEI / Georgia Activities

- SEI Site Visit (July 2019)
- SEI Regional Training & Forum of Incident Response and Security Teams (FIRST) Technical Colloquium (November 2019)
- SEI Remote Network Analysis and Defense Workshop (June 2020)
- Anticipated engagement at FIRST Annual General Meetings and the Annual Technical Meetings of CSIRTs with National Responsibility

Recommendations

- Strengthen cybersecurity legislation and policy.
- Define the role of the national CSIRT and the roles/responsibilities of other cybersecurity stakeholders.
- Develop services and receive tailored training to those services (Incident handling, threat intelligence).
- Formalize Information Sharing processes.
- Develop awareness building programs/campaigns (general public and government system users).

Capacity Building Efforts

Thus far and looking ahead to the future, efforts will be centered around the following key activities:

- Bilateral support and mentorship
- Implementation assistance
- Regional events and training
- Introduction to international communities and best practices

Cybersecurity Capacity Building

Lessons Learned & Best Practices

From the Field

Based upon our experiences and information gathered in the field over the years, the most prominent indicators of an incident response team's success have been:

- establishing long-term relationships with constituents
- their ability to reach many constituents and provide value to them
- their ability to provide actionable information and enable their constituents to be able to react successfully to information security threats
- continued attention and buy-in from national leaders and constituents who continue to report new incidents to them
- their capability to react successfully and in a timely manner to threats and incidents
- their development of ***recognition, credibility, and respect*** from the global and regional community

Best Practices – 1

- Establish a national cybersecurity strategy, policy and a designated National CSIRT.
- Ensure government buy-in and support and the authority or influence needed to engage constituents.
- Garner ***trust*** and prove ***value*** to the constituency (starting with a subset of the constituency and building out over time).
- Adjust services as constituency needs and abilities evolve, and provide services with the most value.
- Routinely gather and analyze constituency feedback.
- Share information, expertise, and specialized capabilities among other teams and sectors within the country.
- Develop regional and global relationships.

Best Practices – 2

- Accurately document policies and procedures that are understood and followed by staff.
- Hire individuals who have a combination of technical and soft skills, analysts at various skill levels.
- Have someone other than the operational manager designated to perform outreach roles.
- Establish plans, funding, and processes for professional development.
- Have the flexibility to select open source tools when they are cost effective options, but evaluate tool needs in conjunction with assessing skills to hire the right staff.

Best Practices - FIRST CSIRT Services Framework

The Forum of Incident Response and Security Teams (FIRST) established a framework for a core set of services that can be leveraged for the selection of services or improvement upon particular functions:

https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Questions?

Contact Us

- Team email: security-operations@cert.org
- For more information: www.sei.cmu.edu

Carnegie Mellon University
Software Engineering Institute
4500 Fifth Ave
Pittsburgh, PA 15213
sei.cmu.edu
info@sei.cmu.edu