Creating a Process Map for Incident Management

CERT® Coordination Center
Networked Systems Survivability
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Presentation Outline

Introduction
Overview of Process Mapping
Process Map for Incident Management
The Future
Project Description

New work being done by the CERT CSIRT Development Team includes the development of an assessment methodology for CSIRTs.

This methodology and resulting assessment instrument will enable teams to evaluate their incident management performance for the following processes: Protect, Prepare, Detect, Triage and Respond.

The project is informally called: The CSIRT Assessment Project.
Project Team Members

CERT CSIRT Development Team Members
• Georgia Killcrece
• Robin Ruefle
• Mark Zajicek

Survivable Enterprise Management Team Members
• Chris Alberts
• Audrey Dorofee

Project Methodology

The project will look at the incident management function in an organization from a risk analysis perspective to determine
• the set of processes required
• possible risks in the performance of those processes
• the impacts if the process fails
• mitigation strategies to avert the failures

Based on this information a set of criteria or requirements against which an organization can benchmark or evaluate their incident management capability will be developed.
Project Requirements

Conform or be applicable to Department of Defense (DoD) Computer Network Defense Service (CNDS) Metrics.

Integrate with Enterprise Security Management (ESM) work being developed within the Software Engineering Institute (SEI) Networked Systems Survivability (NSS) program.

CNDS Metrics -1

The U.S. Department of Defense established directive and instruction whereby all DoD Components are required to establish and provide for computer network defense services (CNDS).

The CND service is built around a framework of functional capabilities that traditionally reside within the mission of the computer security incident response team (CSIRT).

These capabilities fall into general areas of: Protect, Detect, Respond, and Sustain.
CNDS Metrics -2

The primary goal of the DoD CNDS certification and accreditation (C & A) process is to enhance the survivability of DoD information systems and computer networks through a standardized evaluation process.

A secondary goal is to ensure a higher quality of protection service through increased maturity and understanding of CND Services.

The DoD's evaluation process is used as a measurement of mission effectiveness, operational performance, and functional maturity through a number of critical success factors.

Defining Enterprise Security Management

ESM answers the questions:

How can I achieve and sustain a secure state that
• supports achieving enterprise critical success factors?
• increases my organization's resilience in the face of a security incident?
• ensures my organization operates at an acceptable level of security?
• enhances operational excellence?

ESM addresses the protection of critical assets and the effective management of security processes at the enterprise level.
ESM: Foundation Principles

Mobilize enterprise-wide capabilities in a coordinated and collaborative way to achieve and sustain a secure state.

- Focus on key mission requirements by using Critical Success Factors (CSFs)
- Achieving CSFs requires the protection of critical assets
- Protecting critical assets = meeting their security requirements (using defined processes)
- Deploy processes that protect critical assets and achieve critical success factors

ESM: Focus

Enterprise security management focuses on the interaction between assets and processes:

- Assets are valued by the organization and must be protected to achieve the mission
- ESM processes act on these assets to ensure that their security requirements are defined, implemented, measured, and controlled
ESM: Components

Emerging framework that defines the core capabilities necessary to achieve and sustain a secure state

A mobilizing or institutionalizing approach that defines the coordination and cooperation that must exist among the core capabilities

Tools, techniques, and methods that enable the optimization* of the core capabilities to achieve an organization’s desired security state

* To make as effective or functional as possible

Mobilizing to Achieve/Sustain Enterprise Security

Critical Success Factors: determine priorities

ES Governance: policy, oversight, sponsorship

Risk Mgmt: clarifies risk tolerance, impacts

Audit: evaluates

IT Ops: delivers secure service, protects assets

Project Mgmt: plans, tracks, ensures completion

Process Mgmt: enables

Security: defines controls for key IT ops processes
Framework Capability Areas -1

Identification and use of critical success factors to determine organizational priorities

*Enterprise security governance* to define and enforce policy and enact visible sponsorship

*Risk management* to articulate the organization’s risk tolerance and manage risks to critical assets

*Audit* to evaluate the organization’s current state against established criteria

Framework Capability Areas -2

*Project management* to identify, track, and successfully manage ES related projects

*Process management* to define and improve ES process definitions as well as IT processes that implement security

*IT operations* to provide a robust, flexible infrastructure that protects critical assets and delivers secure services

*Security operations* to define security controls and ensure their effective implementation
Integration of EMS and Incident Management

Incident Management is the development of a plan of action, a response plan that
• integrates into the existing processes and organizational structures
• strengthens and improves the capability of the constituency to effectively manage computer security events
• is part of an overall strategy to protect and secure critical business functions and assets
What’s Missing?

CSIRTs need

• a framework, a model, something against which to place and measure themselves (current state), and reference themselves to others
• improvement approaches and a path to reach their desired state
• a coherent, organized community of practitioners and artifacts to help guide the work

History and Rationale

Multiple paths have led us to this project.

• Research
  - State of the Practice Technical Report
  - Organizational Customer Work
• Previous work
  - CSIRT requirements work
  - Courses on Creating and Managing a CSIRT
  - OCTAVE work
  - Survivable Enterprise Management Work
• Future work needs
  - CSIRT framework and methodology
  - CSIRT self-directed evaluation
  - CSIRT best practices
Research Motivations

Questions that need answered

• Where do I start and what steps do I take to create a CSIRT or incident handling capability?
• Where does incident management occur in the organizational enterprise?

Building the Framework

Our Steps include

• incident management process maps
• evaluation instrument
• framework for building and sustaining incident management capabilities
Process Mapping Work Documents and Forms

Brainstorming Notes
Workflow Diagrams
Process Data Templates
Process Interface Templates

Process Data Templates

Fields and data include
- mission and objectives
- triggers for process
- completion criteria
- general policies and rules
- inputs and outputs
- process requirements
- written procedures
- people
- technologies
- other or miscellaneous information or actions
Process Interface Templates

Fields and Data include
- mission and objectives
- triggers for process
- completion criteria
- general policies and rules
- processes involved
- objects being transported or transmitted
- handoff requirements
- written procedures
- sending and receiving actors
- transmitting or transported modes and mechanisms
- other miscellaneous

The CSIRT Process Mapping Project Steps

- brainstormed to initially define the high-level processes
- continued brainstorming sessions to detail each process via 1st and 2nd level workflow diagrams
- coordinated many reviews, revisions, and re-engineering of processes
- completed process data templates and process interface templates for each high level process
- identified risks and impacts for each process (done by smaller team of subject matter experts)
- designed the evaluation instrument based on the risks and impacts (this was also done by the smaller team)
- reviewed and revised the evaluation instrument
Current Status

Top level and secondary level workflow diagrams, process data templates, and process interface templates completed.
Evaluation instrument created.
Technical report in development.
Pilot of evaluation in development.

Presentation Outline

Introduction

» Overview of Process Mapping
Process Map for Incident Management
The Future
Overview of Process Mapping

What is it?

How can it be applied to CSIRT operations?

What is Process Mapping? - 1

A process map defines a set of activities required to accomplish a defined mission.

A process map highlights activity dependencies, interrelationships, and sequencing.
What is Process Mapping? - 2

A process map includes

- goals and objectives
- processes and activities
- inputs and outputs
- roles and responsibilities
- constraints
- enablers
- supporting technology
- procedures and documentation
- interfaces or hand-offs
- interrelationships and dependencies

What is Process Mapping? - 3

<table>
<thead>
<tr>
<th>Work Process Workflow</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Process Dependencies</td>
<td>• Other organizational units • Partners • Suppliers</td>
<td>Work Process</td>
</tr>
<tr>
<td>Work Process Management</td>
<td>• Process organization • Process management</td>
<td>Operational Environment</td>
</tr>
<tr>
<td>• Business environment • Organizational environment • Regulatory environment • Support environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work Process Execution</td>
<td>• People • Process • Technology</td>
<td>Mission and Plan</td>
</tr>
<tr>
<td>• Objectives • Funding profile • Period of performance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is Process Mapping? - 4

It’s a component of business process re-engineering
- identifying core business processes
- mapping the as-is processes
- rethinking the processes

A process is re-engineered to
- increase efficiency or effectiveness
- alter scope
- understand its weaknesses and strengths
- make other improvements

Benefit to CSIRT Operations?

Mapping the CSIRT process
- enables comprehensive understanding of the as-is state
  - completeness
  - strengths and weaknesses
  - interfaces
  - roles and responsibilities
  - dependencies
- identifies risks to successful completion of CSIRT mission
- supports decisions about improvements to CSIRT operations
How Can It Be Applied to CSIRT Operations? -1

Map your CSIRT process through comparison to a “standardized” model of CSIRT best practices

Identify strengths, weaknesses, risks, and compensating factors

- process, technology, people
- interfaces and handoffs
- environmental factors
- operational considerations

Use as a foundation for future improvements

How Can It Be Applied to CSIRT Operations? -2

Can also be used to help benchmark what CSIRT processes an organization already has in place.

This will allow for the determination of current gaps – to help focus any CSIRT development or improvement activities.

Organizations can also use our concepts and processes to do customized mapping.
Presentation Outline

Introduction
Overview of Process Mapping
Process Map for Incident Management
The Future

Process Map for Incident Management

CERT CSIRT Development Team process map for incident management

- Assumptions and rules
- Overview of process components
  - Prepare/Improve/Sustain
  - Protect
  - Detect
  - Triage
  - Respond
- Overview of first level processes
- Applying risk analysis to the process map
Assumptions and Rules

Looking at
- Best practices
- Common practices

Not exceptions
- You can always think up an exception or special situation.
- We tried to exclude these types of processes.

Overview of Process Components

- Prepare/Improve/Sustain
- Protect
- Detect
- Triage
- Respond
Incident Response

Prepare/Improve/Sustain CSIRT

Inputs include
- CSIRT process requirements
- CSIRT process needs

Processes include
- coordinate planning
  - identify CSIRT requirements
  - establish CSIRT vision
  - obtain CSIRT funding and sponsorship
- coordinate implementation
  - develop CSIRT policies, processes, or plans
  - establish CSIRT incident handling criteria
  - implement defined CSIRT resources (staff, equipment and infrastructure)
- evaluate CSIRT capability
- determine CSIRT process modifications
- implement CSIRT process modifications
Protect Infrastructure

Inputs include

- organizational policies
- relevant laws and statutes
- standards, metrics, and best practices

Processes include

- determine infrastructure protection and survivability requirements
- harden and secure infrastructures according to the requirements and continue to carry out changes and improvements as needed
- monitor, assess, and analyze infrastructure for survivability (e.g., monitor network activity and physical access, conduct periodic risks assessments)
- repair and recover from problems, events, or incidents
Sample Guidelines -1

• ISO 17799/British Standards Institute 7799 Part 2
• Control Objectives for Information and related Technology (COBIT)
• Information Technology Infrastructure Library (ITIL)
• National Institute of Standards and Technology (NIST) (selected SP 800 series); FIPS 199
• (ISC)² CISSP Body of Knowledge (International Information Systems Security Certification Consortium; Certified Information Systems Security Professional)
• Federal Financial Institutions Examination Council (FFIEC) Handbooks

Sample Guidelines -2

• Information Systems Security Association; Generally Accepted Information Security Principles (ISSA GAISP)
• Information Technology Governance Institute (ITGI) sources
• National CyberSummit Task Force reports (draft)
• Information Security Forum Best Practices
• SEI body of work including CMM, CMMI, OCTAVE, Security Knowledge in Practice (SKiP℠), CERT Security Practices
Detect

Reactive processes
• notice events
  - constituency member notices unusual activity
  - external sources report activity or events or share advisories and alerts
• receive information

Proactive processes
• monitor indicators
  - monitor networks and hosts
  - proactive vulnerability evaluation
  - public monitoring/technology watch
• analyze indicators

Send notable information to triage.
Triage

Inputs
- event information from detect process
- analysis of indicators from detect process

Processes include
- categorize events
- prioritize events
- assign events
- close events
Respond

Inputs include
- event information
- incident information

Processes include
- receive information
- analyze information
- plan response strategy
- coordinate and respond to incident (coordinate technical, management, and legal response as needed or appropriate)
- close incident (could include as appropriate: document, archive, post-mortem, notify)
R1 Respond to Technical Issues

Decision points include

- decide to perform a post-mortem
- decide if and how to disseminate information
- decide if and how to archive and document information
Next Steps

Develop a gap analysis instrument to help document the “as-is” state of an organization in regards to incident management processes.

Apply risk analysis to incident management processes.

Determine common failure modes for processes.

Determine common mitigation strategies to prevent failure.
Risk Evaluation Process

Risk Data

Identify Risks

Analyze Risks

Prioritized list of risks

Develop Mitigation Strategies

Risks to the CSIRT process

Example of Evaluation Results

Driving Condition
The process is ad hoc. Things sometimes slip through the cracks.

Mitigating Condition
People have extensive experience and skills in monitoring systems and networks.

Risk

Common Failure Mode
Suspicious activity is not detected by proactive monitoring.

Impact: High
Probability: Medium
Common Failure Modes for Detect

- Constituency does not notice unusual or suspicious activity.
- Constituency notices unusual or suspicious activity, but does not report it to the CSIRT.
- Handoff of event reports from constituency to the CSIRT fails.
- Handoff of event reports from constituency to the CSIRT is delayed.
- IT staff does not detect unusual or suspicious activity through proactive monitoring.
- Handoff of event reports from IT staff to the CSIRT fails.
- Handoff of event reports from IT staff to the CSIRT is delayed.
- The CSIRT closes an event that should be forwarded to Triage.

Presentation Outline

Introduction
Overview of Process Mapping
Process Map for Incident Management
The Future
The Future of this Project

Perform a pilot evaluation of the assessment/evaluation instrument.

Develop technical reports (possible titles).
- Creating a Process Map for Incident Management
- Creating a CSIRT Assessment Process
- Evaluating CSIRT Processes and Operations – a Pilot Study

Integrate resulting work into our course materials.

Develop new work.
- Framework for creating and managing a CSIRT
- Corresponding artifacts: templates, checklists, guidelines, forms and process plans

How Can You Participate?

We are looking for collaborators to
- Review and comment on the draft process maps and resulting technical reports and artifacts.
- Help develop new materials and artifacts based on these process maps and the resulting work.
- Possibly serve as pilot sites for the evaluation instrument.
Questions and Comments?

References – Process Mapping

References – CSIRT Information

- Handbook for CSIRTs, Second Edition
- State of the Practice of CSIRTs
  http://www.cert.org/archive/pdf/03tr001.pdf
- Organizational Models for CSIRTs
  http://www.cert.org/archive/pdf/03hb001.pdf
- Forming an Incident Response Team
- Expectations for Computer Security Incident Response
  http://www.ietf.org/rfc/rfc2350.txt
- Computer Security Incident Handling Guide, National Institute of Standards and Technology (NIST SP 800-61)

Contact Information

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA
Web: http://www.cert.org/
Email: cert@cert.org
Hotline: +1 412 268 7090
CERT personnel answer
08:00–17:00
EST(UTC-5)/EDT(UTC-4)
On call for emergencies during other hours

CERT CSIRT Development Team
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA
Web: http://www.cert.org/csirts/
Email:
Chris Alberts
cja@sei.cmu.edu
Audrey Dorofee Robin Ruefle
ajd@sei.cmu.edu rmr@cert.org
Georgia Killcrece Mark Zajicek
georgia@cert.org mtz@cert.org