

Creating and Managing Computer Security Incident Handling Teams (CSIRTs)

CERT Training and Education

Networked Systems Survivability
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

This material is approved for public release.

Distribution is limited to attendees by the Software Engineering Institute.

CERT, CERT Coordination Center, and Carnegie Mellon are registered in U.S. Patent and Trademark Office by Carnegie Mellon University



This work is sponsored by the Office of the Under Secretary of Defense (Acquisition and Technology), U.S. Department of Defense.

© 2008 Carnegie Mellon University.

Requests for permission to reproduce these materials or to prepare derivative works of these materials for other than government purposes should be addressed to the SEI Licensing Agent or sent to permission@sei.cmu.edu.

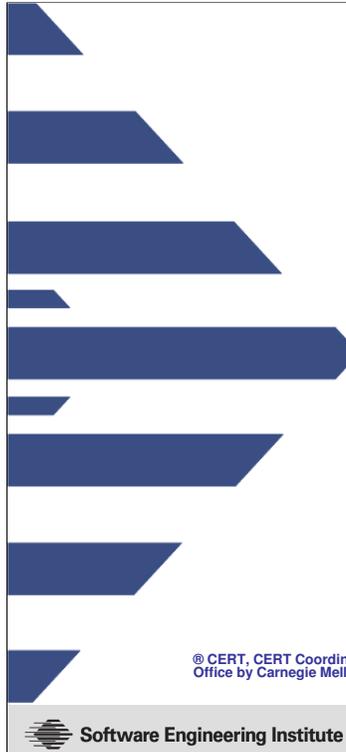
NO WARRANTY

This Carnegie Mellon University and Software Engineering Institute material is furnished on an “as-is” basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

This work was created in the performance of Federal Government Contract Number F19628-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for United States government purposes pursuant to the copyright license under the clause at 52.227-7013.

Use of any trademarks in these materials is not intended in any way to infringe on the rights of the trademark holder.

CERT, CERT Coordination Center, and Carnegie Mellon are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.



Creating and Managing Computer Security Incident Response Teams (CSIRTs)

Georgia Killcrece and Robin Ruefle
CSIRT Development Team
CERT® Program
Software Engineering Institute
Carnegie Mellon University

© CERT, CERT Coordination Center, and Carnegie Mellon are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

 **Software Engineering Institute** | CarnegieMellon © 2008 Carnegie Mellon University

The CERT® Program is part of the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. Following the Morris worm incident, which brought 10 percent of internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. This center was named the CERT Coordination Center (CERT/CC). While we continue to respond to major security incidents and analyze product vulnerabilities, the role of the CERT/CC has expanded over the years. Along with the rapid increase in the size of the internet and its use for critical functions, there have been progressive changes in intruder techniques, increased amounts of damage, increased difficulty of detecting an attack, and increased difficulty of catching the attackers. To better manage these changes, the CERT/CC is now part of the larger CERT Program, whose primary goals are to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of successful attacks, accidents, or failures ("survivability").

Broad areas of work being done within the CERT Program include Vulnerability and Incident Analysis, Survivable Enterprise Management, Education and Training, Survivable Systems Engineering, Network Situational Awareness, Community Involvement. More information about each of these areas can be found at http://www.cert.org/meet_cert/meetcertcc.html.

CERT is chartered to work with the internet community in detecting and resolving computer security incidents, as well as taking steps to prevent future incidents. In particular, our mission is to

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Facilitate communication among experts working to solve security problems.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Maintain close ties with research activities and conduct research to improve the security of existing systems.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.

Creating and Managing CSIRTs Agenda

Introduction

Defining Incident Management (IM)

Defining CSIRTs

Creating an Effective CSIRT

CSIRT Components

IM Processes and Operational Best Practices

Summary



Introduction

Defining incident management

- Incident management as a risk management activity
- Incident management and control capability in REF

Defining CSIRTs

- What is a CSIRT?
- What Does a CSIRT do?
- General Categories of CSIRTs

Creating an Effective CSIRT

- Implementation Recommendations

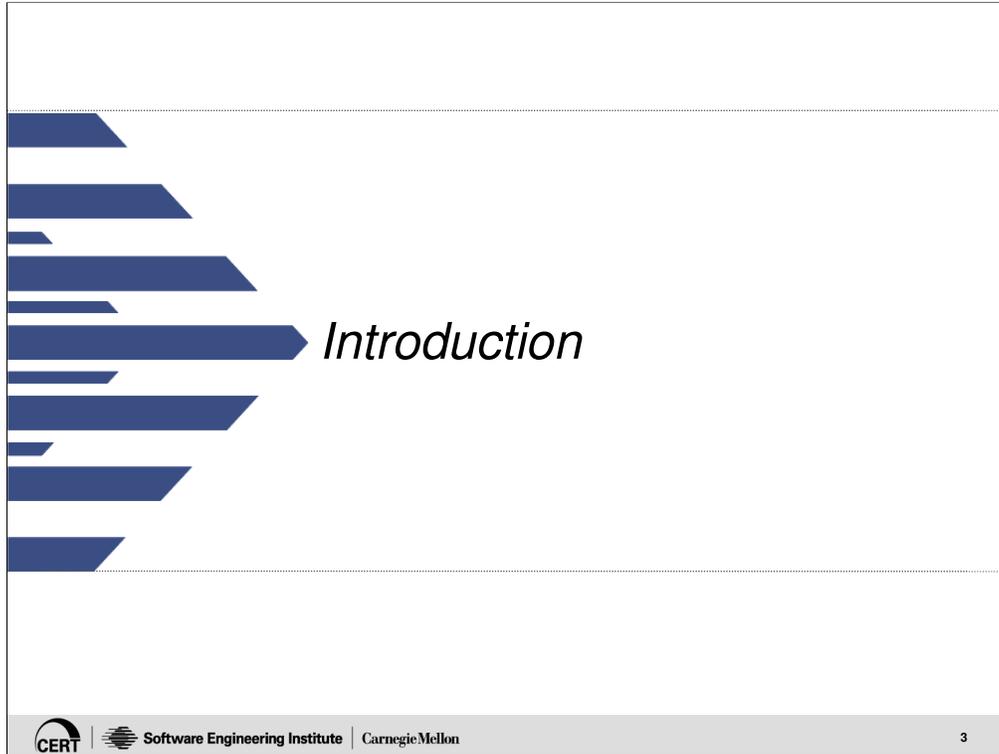
CSIRT Components

- Constituency and Mission
- Funding and other organizational Issues
- Services and supporting policies and procedures
- Resources (staff, equipment, infrastructure)

Incident Management Processes and Operational Best Practices

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

Summary



Some key definitions:

- constituency - a defined group supported by your CSIRT; could be multiple commercial organizations, one parent organization, or organizations within a particular geographic region, etc.
- organization - the organization in which your CSIRT is housed, often called parent organization or host organization.

Tutorial Goals

This tutorial will look at the CSIRT role and function within an enterprise incident management capability.

It will present a high level overview of

- management
- organizational
- procedural
- operational

issues involved with creating and operating a Computer Security Incident Response Team (CSIRT).

Specific topics discussed will include CSIRT

- benefits and limitations
- requirements and framework
- variety and level of services
- common policies and procedures
- communications and collaboration
- operational best practices



The session will provide a high-level view into the type of work that CSIRT managers and staff may be expected to handle. It also provides an introduction to the incident handling process and the nature of incident response activities. Specific topics covered will include

- building an enterprise incident management capability
- managing the CSIRT infrastructure
- protecting CSIRT data
- hiring CSIRT staff
- coordinating response

This tutorial will also present a best practice model for performing incident management and discuss incident management activities and how some activities may be provided by other members of an organization beyond those provide by a CSIRT.

Intended Audience

Individuals tasked with creating a CSIRT or incident management capability.

Computer Security Incident Response Team (CSIRT) staff, including managers who are

- prospective
- new
- existing

Other individuals who need or would like an understanding of CSIRT management issues

Individuals interested in learning more about CSIRTs and incident management activities in general



This tutorial is designed to provide managers and other interested staff with an overview of the issues involved in creating and operating a CSIRT, as well as the decisions that must be made to ensure that your CSIRT staff is providing appropriate services to your CSIRT constituency.

Individuals tasked with creating a CSIRT might include

- chief information officers (CIOs)
- chief security officers (CSOs)
- managers
- project leaders
- project team members
- other personnel involved in incident management activities that interface with the CSIRT

Other staff who may be interested in finding out more about CSIRT operations might include

- legal staff, human resources
- existing security staff, system and network administrators
- public relations staff
- business owners/operators
- mid-level or senior management, risk management and audit staff
- business continuity, business resumption, disaster recovery staff
- constituency members
- outsourcing partners, managed security service providers

No previous incident-handling experience is required for this tutorial.

Applying This Material

All CSIRTs are different.

- One size does not fit all.

Take what makes sense for your situation.

- Your mileage may vary.



Each organization must decide the structure and operation that works for them.

Not all CSIRTs are created equal, solutions that work for one team may not work for another because of various constraints and environmental situations.

Look at what works for your organizational mission and goals.

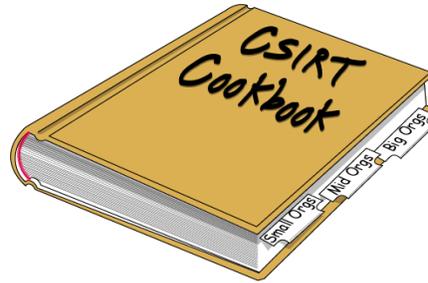
Recognize that some techniques and operational methodologies will only be learned with time and experience.

There is No Single Recipe

There is no single recipe for creating a CSIRT.

It depends on your

- needs and requirements
- mission and goals
- available resources and support

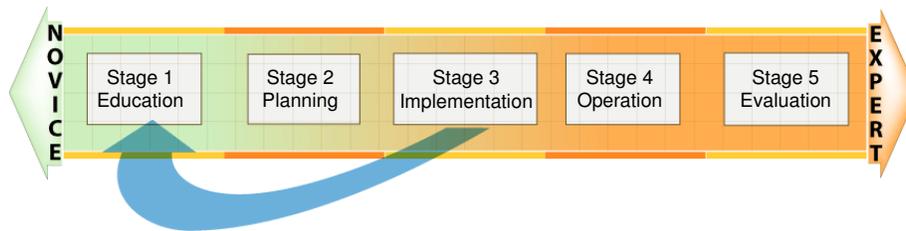


There is no recipe to follow to create an effective CSIRT.

This tutorial identifies the ingredients - but you must determine how to mix those ingredients together in a formula that works for your organization and constituency.

Stages of CSIRT Development

- Stage 1 Educating the organization
- Stage 2 Planning effort
- Stage 3 Initial implementation
- Stage 4 Operational phase
- Stage 5 Evaluation and improvement



This slide represents the typical stages we see in the development of a CSIRT.

In Stage 1, the organization wants to start a team or build an incident management capability but does not really understand incident management functions or know what a CSIRT is or does. The organization needs to go through some awareness training to learn about various approaches for implementing a capability.

In Stage 2, the organization has some knowledge about CSIRTs, and is beginning to identify and analyze the various issues that must be addressed to plan the CSIRT implementation.

In Stage 3, the CSIRT exists in some form and begins to provide services. It has identified its constituency, defined a mission and set of services, hired initial staff and provided training, drafted a set of standard operating procedures (SOPs), and has set up a secure infrastructure. It is also beginning to communicate and interface with members of the constituency and other interfaces.

In Stage 4, the CSIRT is handling incidents and has been operational for six months to one year. It is a peer collaborator with other CSIRTs.

In Stage 5, the CSIRT is a mature team. It has been in existence for two years or more, and has extensive experience in incident handling. The CSIRT now looks for ways to improve its incident management capability. It may do this by evaluating its operations, identifying strengths and weaknesses, and planning improvements based on its mission, available funding, and available resources.

One important point to stress is that a team can be at an advanced stage but still need to step back and revisit some of the early stages to validate that the right issues are being addressed, to recycle through planning or implementation changes should there be organizational restructuring or changes in reporting requirements, or if there are changes in staffing, funding or missions, services, etc.



Defining incident management

- relationship to incident response
- incident management as a risk management and operational resiliency function

The Risks

While the Internet is revolutionizing the way we do business, the risks the Internet introduces can be fatal to a business.

Network attacks have resulted in

- Unauthorized release of personal data
- Identity theft
- High tech bank robbery
- Loss of intellectual property
- Massive disruption of service
- Medical records tampering
- Extortion to avoid disruption or exposure of sensitive information



Computer networks have revolutionized the way business is done, but have also introduced substantial risks.

Network attacks can lead to lost

- lives
- money or profit
- products
- sensitive or proprietary information
- personnel data
- reputation and branding

Why is Internet security a problem?

There exists a multitude of security vulnerabilities in systems and applications available on the Internet. Many of these vulnerabilities are exploitable through the Internet, because security was not a primary consideration in the design of Internet protocols.

The Internet was originally designed as a research project to share information and resources. It was created by a small group of researchers who knew each other. The goal was to be able to get to various resources and information remotely. Keeping people out or restricting access to resources was not something that was needed.

Furthermore, the complexity and administration of computer and network infrastructures makes it even more difficult to properly manage the security of computer and network resources. As a result there are many more computer security events or incidents occurring. Network and system administrators do not always have the people and practices in place to defend against attacks and minimize damage.

Legal Compliance Issues Must Now Be Addressed

New rules and regulations are being introduced to ensure *data protection, privacy, and accountability*.

This can have an impact on the security policies and procedures required for an organization, especially as they relate to

- data protection requirements
- incident response capabilities
- notifications of unauthorized access to data



Some U.S. examples include

- Gramm-Leach-Bliley Act of 1999 (GLBA, also known as the Financial Services Modernization Act of 1999) – requires financial institutions to have customer privacy policies and an information security program.
- Health Insurance Portability and Accountability Act (HIPAA) – requirements include securing the privacy and integrity of health information for certain types of health organizations.
- Federal Information Security Management Act (FISMA) – which is part of the E-Government Act of 2002 states that all U.S. federal government agencies are responsible for ensuring the information security of their systems, including performing annual independent evaluations. Under FISMA, all U.S. federal agencies are also required to establish an incident response capability and procedures for detecting, reporting, and responding to security incidents.
- Sarbanes-Oxley Act of 2002 – mandates the implementation and evaluation of internal controls for data and information used in financial reporting, this includes information on the storage, protection, and length of retention of electronic records.
- State Security Breach Notification Laws – As of 2007, 39 states have enacted laws which require businesses, nonprofits, and state public institutions to notify consumers when their personal information has been compromised. Nine (9) other states have introduced similar legislation.
<<http://www.pirg.org/consumer/credit/statelaws.htm#breach>>
<<http://www.ncsl.org/programs/lis/cip/priv/breach.htm>>

International examples

- Canada's Personal Information Protection and Electronic Document Act
- European Union's Privacy Directive
- Japan's Personal Data Protect Act
- U.K. Data Protection Act
- Basel II Guidelines

Insider Threats Are Still a Problem

The following information represents the major findings observed across the **insiders** and incidents studied in the **banking** and **finance** sector.

- Most incidents required little technical sophistication.
- Perpetrators planned their actions.
- Financial gain motivated most perpetrators.
- Perpetrators did not share a common profile.
- Incidents were detected by various methods and people.
- Victim organizations suffered financial loss.
- Perpetrators committed acts while on the job.



In 2004 U. S. Secret Service and CERT/CC published a report on insider threats in the banking and finance sector based on research conducted jointly by both groups. This report draws on case records, investigative reports, and interviews, it analyzes technical and behavioral indicators for the early detection of illicit cyber activity by organizational insiders. The report, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, can be found at: <http://www.cert.org/archive/pdf/bankfin040820.pdf>

The report examines 23 incidents carried out by 26 insiders in the banking and finance sector between 1996 and 2002. Some of the statistics from the report include

- In 87% of the cases studied, the insiders employed simple, legitimate user commands to carry out the incidents. In only a small number of cases was a more technical knowledge of network security required.
- In 70% of cases studied, the insiders exploited or attempted to exploit systemic vulnerabilities in applications and/or processes or procedures (e.g., business rule checks, authorized overrides) to carry out the incidents.
- In 78% of the incidents, the insiders were authorized users with active computer accounts at the time of the incident. In 43% of the cases, the insider used his or her own username and password to carry out the incident.
- In 85% of the incidents, someone other than the insider had full or partial knowledge about the insider's intentions, plans, and/or activities, including co-workers, friends and family members.
- Insiders ranged from 18 to 59 years of age. 42% of the insiders were female. Insiders came from a variety of racial and ethnic backgrounds and were in a range of family situations, with 54% single and 34% married.
- Only 17% of the insiders had system administrator/root access prior to the incident.
- In 61% of the cases, the insiders were detected by persons who were not responsible for security, including customers (35%), supervisors (13%), and other non-security personnel (13%).
- In 22% of the cases, insiders were caught by auditing or monitoring procedures; 26% were caught through system failures or irregularities, and 61% by manual procedures, including an inability to log in, customer complaints, manual account audits, and notification by outsiders.

Framing the Problem

The speed with which an organization can recognize, analyze, and respond to an incident will limit the damage done and lower the cost of recovery.

Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen.

When information or technology incidents occur, it will be critical for an organization to have an effective means of responding.



Changes in

- organizational data protection requirements
- institutional regulations and local or national laws
- intruder technology

have made it imperative to address security concerns at an enterprise level.

Other motivators driving the establishment or formalization of incident management processes include

- a general increase in the number of information technology incidents being reported and in the number and type of organizations being affected by such incidents
- a more focused awareness on the need for security policies and practices as part of their overall risk-management strategies

Strategies for Effective Response

Organizations require a multilayered approach to secure and protect their critical assets and infrastructures.

As a defense against Internet and internal risks and threats, organizations can

- identify key assets and data and their location, business owners, and criticality
- perform risk assessments
- keep up to date with the latest operating system patches and product updates
- install perimeter and internal defenses such as routers, firewalls, scanners, and network monitoring and analysis systems
- update and expand information technology and security policies and procedures
- provide security awareness training to employees, customers, and constituents
- formalize an incident management process



Organizations require a multilayered approach to secure and protect their critical assets and infrastructures. This multilayered strategy requires that not only technical but also organizational and procedural approaches be in place to manage information technology incidents as part of the goal of achieving an enterprise's business objectives in the face of risks and attacks. Organizations, today, want to not just survive attacks but be resilient to whatever malicious activity may occur.

Together these strategies form the basis of an enterprise-wide incident management plan.

What is Incident Management?

The ability to provide end-to-end management of events and incidents across the enterprise that affect information and technology assets within an organization.



For incident response to occur in an effective and successful way, all the tasks and processes being performed must be viewed from an enterprise perspective, no matter who is performing the work. This means identifying how

- tasks and processes relate
- information is exchanged
- actions are coordinated

Understanding this bigger picture of activity and the relationships across the organization is what we mean by incident management.

Identifying and defining these interfaces and the roles and responsibilities of the various participants across the enterprise is a key part of setting up any incident management process or capacity. As an example, looking just at the response part of the process misses key actions that, if not done in a timely, consistent, and quality-driven manner, will impact the overall response. This could possibly delay actions due to the confusion of roles and responsibilities, ownership of data and systems, and authority. Response can also be delayed or ineffective as a result of communications problems (not knowing whom to contact) or due to poor quality of information about an event or incident. Any impact on the response timeliness and quality could cause further damage to critical assets and data during an incident.

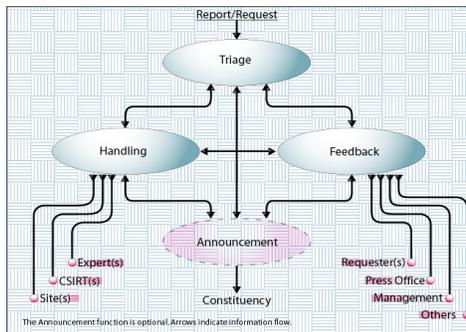
Incident management, then, can be seen as an abstract, enterprise-wide capability, potentially involving every business unit within the organization. It can be viewed as a subset of the organization's broader security, risk, and IT management activities and functions. It can often cross into general security and IT management tasks and practices.

Technology Versus Process

Incident management is not just the application of technology to resolve computer security events.

Incident management requires the development of a plan of action, a set of processes that are

- consistent
- repeatable
- quality-driven
- measurable
- and understood across the constituency or enterprise



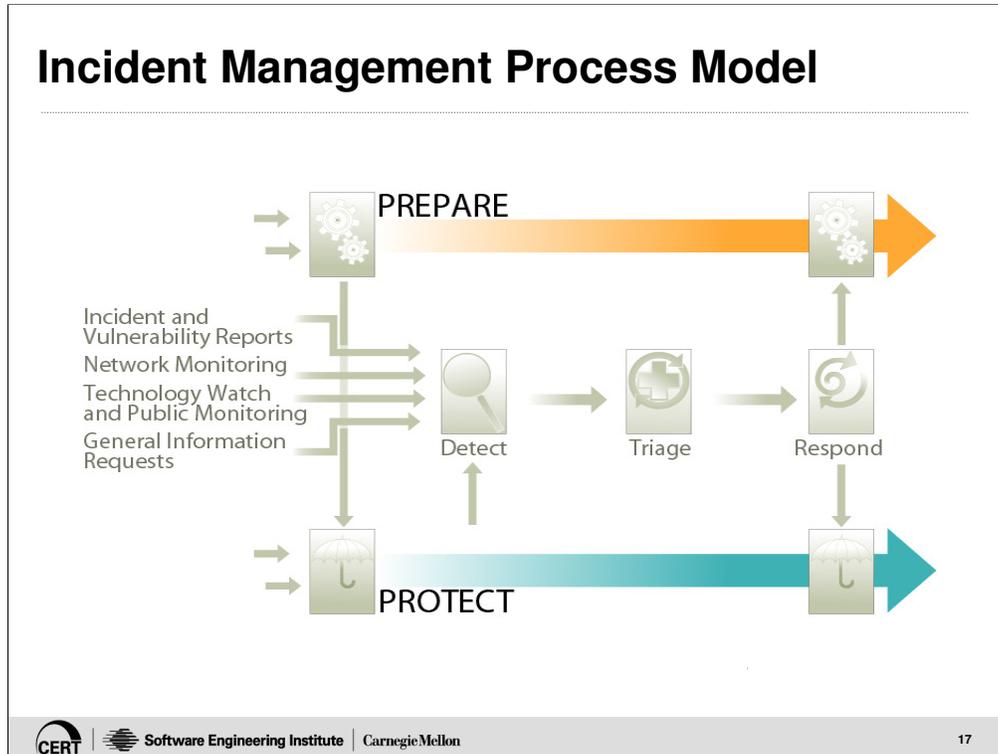
To implement such a plan, we believe organizations need to have quality strategies and processes in place to not only handle incidents that do occur but to also prevent incidents from occurring or re-occurring. These include processes to

- plan and implement a computer security incident management capability
- secure and harden the enterprise infrastructure to help prevent incidents from occurring or to mitigate an ongoing incident
- detect, triage, and respond to incidents and events when they occur

To be successful this plan should

- integrate into the existing processes and organizational structures so that it enables rather than hinders critical business functions
- strengthen and improve the capability of the constituency to effectively manage security events and thereby keep intact the availability, integrity, and confidentiality of an organization's systems and critical assets, where required
- support, complement, and link to any existing business continuity or disaster recovery plans where and when appropriate
- support, complement, and provide input into existing business and IT policies that impact the security of an organization's infrastructure
- implement a command and control structure, clearly defining responsibilities and accountability for decisions and actions
- be part of an overall strategy to protect and secure critical business functions and assets
- include the establishment of processes for
 - notification and communication
 - analysis and response
 - collaboration and coordination
 - maintenance and tracking of records

Incident Management Process Model



The CSIRT Development Team in the CERT Program has defined a “best practice” set of processes for incident management.

To do this we

- determined processes
- outlined processes via workflow diagrams
- provided details and requirements of each process

This model is presented and described in SEI Technical Report CMU/SEI-2004-TR-015, *Defining Incident Management Processes: A Work in Progress*. This report is available at:

- <http://www.cert.org/archive/pdf/04tr015.pdf>

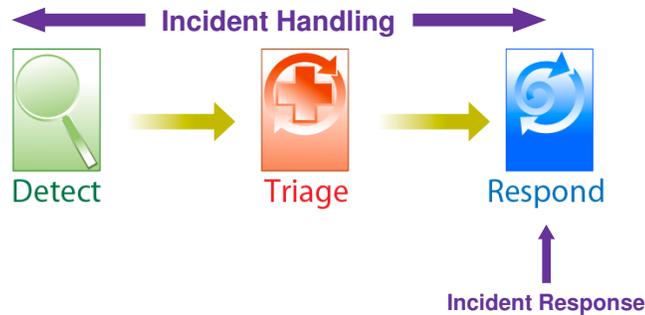
This model documents a set of processes that outline various incident management functions. From this work a methodology for assessing and benchmarking an organization’s incident management processes can be developed. This methodology and resulting assessment instrument will enable teams to evaluate their incident management performance for the following processes:

- Prepare/Improve/Sustain (Prepare)
- Protect Infrastructure (Protect)
- Detect Events (Detect)
- Triage Events (Triage)
- Respond.

Defining the Terms

What is the definition and what is the difference?

- incident management
- incident handling
- incident response



Throughout the rest of this tutorial, the terms incident response, incident handling, and incident management refer to incidents impacting information and technology assets. The processes and concepts discussed here, however, can also be applied to incident management activities for the other assets.

We define incident handling as one service that involves all the processes or tasks associated with “handling” events and incidents. Incident handling includes multiple functions:

- detecting and reporting – the ability to receive and review event information, incident reports, and alerts
- triage – the actions taken to categorize, prioritize, and assign events and incidents
- analysis – the attempt to determine what has happened, what impact, threat, or damage has resulted, and what recovery or mitigation steps should be followed. This can include characterizing new threats that may impact the infrastructure.
- incident response – the actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to stop the incident from happening again

Incident response, as noted in the list above, is one process, the last step, that is involved in incident handling. It is the process that encompasses the planning, coordination, and execution of any appropriate mitigation and recovery strategies and actions.

Incident management is the larger process that includes incident handling, but adds on the functions of preparing for incident handling work, evaluating and sustaining the functions, and interfacing with other security and risk management activities.

Incident vs. Security Management

Security management is an operational risk management activity.

Incident management is a security management activity.

Incident management is an operational risk management activity.

Security has been redefined as

- a business issue
- owned by the organization
- an investment
- an enterprise process that can be measured and managed

Risk management focuses on keeping critical objects or assets productive by

- limiting risk
- managing the impact of realized risk.

The goal of security is to help attain and sustain operational resiliency.



There is a movement away from a technology-centric, ad hoc, reactive means of managing security (without process and procedures) to an organization-centric, strategic, adaptive, process-centric means.

Risk management focuses on keeping critical objects or assets productive by limiting risk and managing the impact of realized risk.

Operational resiliency is managing operational risk to ensure mission viability by

- being able to adapt to new risks as they emerge
- acting before reacting

For an organizations it means being able to draw upon the capabilities of the entire organization so that they can be deployed to solve an organizational problem. However, because security isn't a point in time activity, it also means being able to do it in a way that is sustainable—systematic, documented, repeatable, optimized, and adequate in the context of the organization's strategic drivers. Otherwise, there is a chance that security activities and resources are misdirected, unable to achieve goals, and unable to know when they have success or failure.

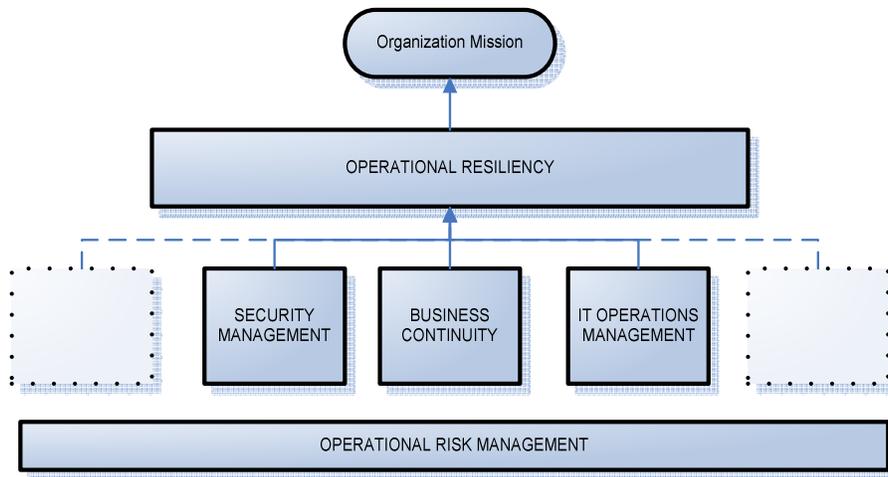
One of the most common complaints about security in organizations is that it is an activity that directly cuts into the organization's bottom line. Unless security is managed in a way that supports and sustains the organization's strategic drivers, this cannot be remedied. Moving security from an expense or sunk cost for the organization to one that is an investment in the organization's long-term viability and resiliency gives security activities purpose and value.

Because resiliency is a function of risk management, and security is a risk management activity, security contributes to operational resiliency through the risk management link.

Moving from "security" to "resiliency" means moving from

- managing to threats and vulnerabilities to managing to impact and consequence
- having no articulated desired state to adequate security being defined as the desired state
- throwing technology at the problem to implementing security in sufficient balance to cost and risk.

Common Goal: Operational Resiliency



Operational risk is the risk that results from

- failed internal processes
- inadvertent or deliberate actions of people
- problems with systems and technology
- external events

Operational resiliency is the organization's ability to sustain the mission in the face of these risks.

Operational resiliency depends on effective management of core operational risk management activities.

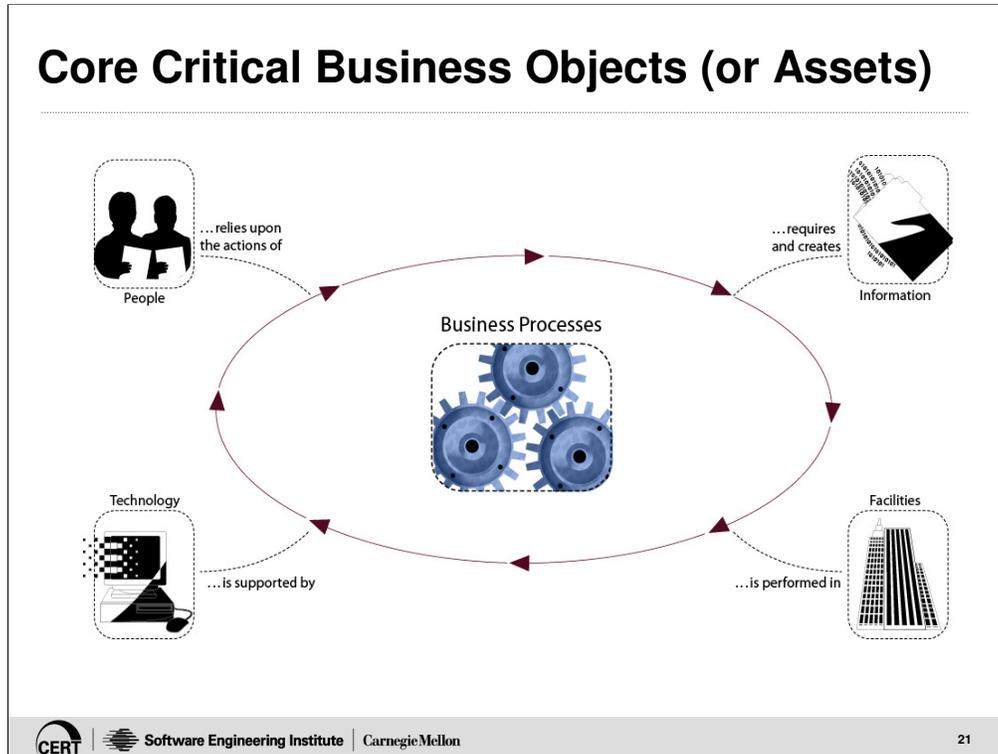
- **security** or **security management** is one activity
- others are **business continuity** and **IT operations management**

Members of the CERT Program's Security Enterprise Management group have been working the past two years with the Financial Services Technology Consortium to identify mature practices in banking and financial services industries. Research and development in this area has produced the CERT® Resiliency Engineering Framework (REF).

For more information on REF, keep your eye on the CERT web site, enterprise security management area:

<http://www.cert.org/esm/>

Core Critical Business Objects (or Assets)



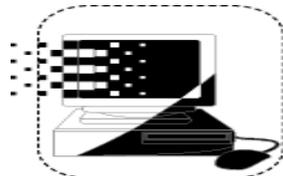
Operational resiliency keeps the operational capacity of the organization from disruption.

The five items in the graphic above signify core critical business objects or assets.

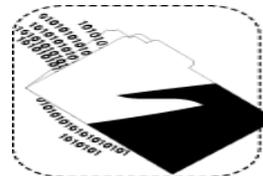
- People are the human capital of the organization. Disruptions to human resources often result in the failure of business processes to achieve their mission.
- Information – is one of the most important assets of the organization, business processes cannot operate effectively without access to information. Disruption of availability of information (either through modification, loss, or destruction) directly affects enterprise resiliency.
- Technology – directly supports the automation of critical business processes, it is pervasive across all functions of the organization. It has a high exposure to risk that can affect the viability of other resiliency objects such as information and facilities.
- Facilities – the physical places where other objects “live”, provides direct support for business process achievement.

Our Focus in this Tutorial

Incident management for this tutorial focuses on handling incidents involving two of the critical objects or assets in an organization:



technology



information

And the business processes they support



Historically we have used the term “computer security incidents” and “computer security incident management” But in this new paradigm for security, those terms can be limiting, confusing, and ambiguous. What we really are talking about are any type of incidents that affect the information or technology and the business processes they support within an organization.

In the REF module, the IMC capability defines an “incident” in the broad terms used in ISO 27002, code of practice for Information Security Management System and the Information Technology Infrastructure Library (ITIL), meaning, any type of incident.

Our focus is on a subset of incidents, information security or information technology incidents. However, the processes defined in the ISO Information Security Management System code of practices and the ITIL model, still apply.

The CERT Resiliency Engineering Framework (REF)

A framework of practice for integration of security and business continuity activities toward achievement and management of operational resiliency (OR).

Defines basic process areas and provides guidelines for security and BC/DR process improvement.

Captures vital linkages between security, BC/DR, and IT ops in the process definition.

Addresses operational risk management through process management.

Establishes a set of benchmarks for 21 different capability areas.

To achieve and sustain OR requires mastery of a variety of competencies.

Operational resiliency emerges from how well these activities are coordinated and executed toward a common goal.



This is a partial list of the competencies.

Enterprise Management

- COMM – Communications
- COMP – Compliance Management
- EF – Enterprise Focus
- FRM – Financial Resource Management
- HRM – Human Resource Management
- OTA – Organizational Training and Awareness
- RISK – Risk Management

Engineering

- RRD – Resiliency Requirements Development
- RRM – Resiliency Requirements Management
- AM – Asset Definition and Management
- CM – Controls Management
- RAD – Resilient Asset Acquisition and Development

Operations Management

- EXD – External Dependencies
- AM – Access Management
- ID – Identity Management
- IMC – Incident Management and Control
- SAP – Scenario Analysis and Planning
- VAR – Vulnerability Analysis and Resolution
- EC – Environment Control
- ISR – Integrated Service Resiliency
- KM – Knowledge and Information Management
- PM – People Management
- Technology Management [TM]

Process Management

- MA – Measurement and Analysis
- MON – Monitoring

Incident Management and Control Capability

Incident management and control capability (IMC), within the REF

- is a risk management activity
- is foundational to managing the security and resiliency of an organization's critical assets and business processes

The organization must establish processes for detecting, analyzing, responding to, and learning from incidents to

- prevent the impact of unanticipated risks
- manage their impact when realized
- provide a source of knowledge to improve
 - protection strategies
 - continuity and sustainability plans and practices

The definition of an incident within this context is very broad, it can relate to anything that disrupts achieving the mission.

Having a better response process in place enables a higher level of operational resiliency.



The Incident Management and Control capability focuses the organization's attention on the life cycle of an incident – from event detection to analysis to response. The organization establishes the incident management plan and program and assigns appropriate resources. Event detection and reporting capabilities are established and the organization sets criteria to establish when events become incidents that demand the organization's attention. Events are triaged and analyzed, and incidents are validated. Supporting activities such as communication, logging, and tracking events and incidents and preserving event and incident evidence are defined and established. Most importantly, the organization performs post-incident review to determine what can be learned from incident management and applied to improve protection and sustainability strategies as well as improvements in the incident management process and life cycle management.

Incidents affect the productivity of the organization's assets, and in turn, associated services. Because assets span physical and electronic forms, incidents can be either cyber or physical in nature, depending on the target of the incident. In the case of "information" and "technology" assets, incidents can be cyber (such as unauthorized access to electronic information or to technology components) or physical (such as unauthorized access to paper or other media on which information assets are stored or to technology assets that are physically accessible.)

The IMC sub-processes include:

- incident planning and assignment of resources
- event and incident detection, identification, and reporting
- incident analysis
- incident response and recovery
- incident learning and knowledge management.

Relationships With Other Capabilities

The IMC capability in the REF Framework does not stand in isolation, it works in conjunction with various other capabilities.

These include

- service continuity
- compliance management
- monitoring
- vulnerability analysis and resolution

There are also parts of some capabilities that support IMC such as

- communications
- organizational training and awareness

When you are building an incident management process and capability, you must look at these other areas and ensure that the right coordination and collaboration occurs between these areas.



Service continuity management deals with developing, testing, and implementing continuity of operations plan.

Compliance management deals with reporting incidents according to applicable laws, rules, and regulations.

Monitoring relates to the processes for identifying and detecting events that could become incidents.

Vulnerability analysis and resolution deals with identifying, analyzing, and managing vulnerabilities in an organizations' operating environment.

The above four capabilities are related because information comes into or out of the IMC capability from these other capabilities.

For example, if during the analysis and response to an incident, there is a policy that the incident needs to be reported to another organization, the process established in the compliance management would be triggered and followed. Same with the service management capability, if a COOP needed to be implemented, then a trigger from the IMC would go to follow the process for implementing the COOP.

Both vulnerability analysis and resolution and monitoring capabilities provide input to the IMC capability. Vulnerability scanning, risk assessments, and network monitoring not only can detect and identify events and incidents but can also provide additional information or evidence for activity that can be analyzed to determine the scope and impact of any incident.

Another View: IMC Metrics

Incident Management Capability Metric Service Categories

Protect	Detect	Respond	Sustain
Risk Assessment Support	Network Security Monitoring	Incident Reporting	MOUs and Contracts
Malware Protection Support	Indicators, Warning, and Situational Awareness	Incident Response	Project/Program Management
CND Operational Exercises		Incident Analysis	CND Technology Development, Evaluation and Implementation
Constituent Protection Support and Training			Personnel
Information Assurance/Vulnerability Management			Security Administration
			CND Information Systems
			Threat Level Implementation



Here is another way to look at the related components that must be taken into account when defining your Incident Management processes and capabilities. In determining what you need to create an incident management capability, you must understand what areas comprise that capability.

We've mentioned some components as identified by the REF Framework and also the Incident Management Process Model.

Another tool that can be used to help structure your incident management capability or CSIRT is the Incident Management Capability (IMC) Metrics.

The purpose of the metrics is to provide organizations with a method for evaluating the effectiveness of their incident management (IM) or computer security incident response team (CSIRT) capability. Because the metrics list various components that must be evaluated to determine the effectiveness of a capability, they can also be used as a roadmap to identify various functions that if not provided by the IMC or CSIRT then must be coordinated with it.

These metrics were adapted from the

- United States Computer Emergency Readiness Team (US-CERT) "Federal Computer Network Defense (CND) Metrics"
- Department of Defense (DoD) 8530 Directive and Instruction for Certification and Accreditation of Computer Network Defense Service Providers (CNDSP), Evaluator's Scoring Metrics

The Incident Management Capability Metrics document can be found at

<http://www.cert.org/archive/pdf/07tr008.pdf>

Who Performs Incident Management?

Incident management functions could be performed by

- CSIRT staff and manager
- IT staff
- physical security staff
- subject matter experts
- vendors
- ISPs/network service providers
- members of the CSIRT constituency
- victims or involved sites
- other CSIRTs or coordination centers
- upper management
- business function units
- HR staff
- PR staff
- auditors, risk management staff, compliance staff
- legal counsel for constituency or CSIRT
- inspector generals
- attorney generals
- law enforcement
- criminal investigators
- forensics specialists
- managed service providers



Based on organizational mission and assigned job responsibilities for incident management, the Respond process could be performed by a variety of personnel.

Responding to computer security incidents does not happen in isolation. Actions taken to prevent or mitigate ongoing and potential computer security events and incidents can involve tasks performed by a wide range of participants; this can include network and system administrators, human resources, public affairs, information security officers (ISOs), C-level managers (such as chief information officers [CIOs], chief security officers [CSOs], chief risk officers [CROs], and other similar types of managers) and even constituent representatives.

This question is one that is often asked by organizations as they plan their incident management strategy. They want to know what organizational units should be involved, what types of staff will be needed to perform the functions, and what types of skills that staff must have. They also want a way to identify what organizational units are already doing this type of work and want to understand the critical interfaces and interactions between different parts of the organization, different security functions, and the incident management process, in an effort to be able to build effective capabilities.

Institutionalizing Incident Management Capabilities

Some organizations may assign responsibility for this function to a defined group of people or a designated unit such as a CSIRT.

This can be seen in organizations such as

- local, state, or provincial governments
- educational institutions or research networks
- national initiatives

Some organizations may perform this function as part of other security, IT, risk management, or business continuity functions.

This is common in commercial industry where this function may be served by

- security teams
- crisis management teams
- resiliency teams

Some organizations may outsource this capacity.



How a computer security incident management capability is instituted within an organization can differ greatly.

For the rest of these materials when we speak about CSIRTs we are speaking in general about all these different kinds of entities that may be involved in performing part of the computer security incident management functions.



Defining CSIRTs

CERT | Software Engineering Institute | Carnegie Mellon 29

What is a CSIRT?

An organization or capability that provides services and support, to a defined constituency, for preventing, handling and responding to computer security incidents



At a more granular level, some incident management functions may be carried out by a Computer Security Incident Response Team—a CSIRT.

A CSIRT is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility of providing part of the incident management capability for a particular organization. When a CSIRT exists in an organization, it is generally the focal point for coordinating and supporting incident response.

CSIRT work is very similar to emergency response work in other sectors. Not only do you need to have the necessary tools and plans in place to respond effectively, but you also must perform other proactive functions to prevent disasters from happening, where possible. So for example, first responders to terrorist attacks, spend time testing their response plans and educating the public on suspicious behavior and how to report it.

Another type of emergency response that illustrates proactive and reactive tasks is a fire department. Part of a CSIRT's function can be compared in concept to a fire department. When a fire occurs, the fire department is called into action. They go to the scene, review the damage, analyze the fire pattern, and determine the course of action to take. They then contain the fire and extinguish it. This is similar to the reactive functions of a CSIRT. A CSIRT will receive requests for assistance and reports of threats, attacks, scans, misuse of resources, or unauthorized access to data and information assets. They will analyze the report and determine what they think is happening and the course of action to take to mitigate the situation and resolve the problem.

Just as a fire department can be proactive by providing fire-prevention training, instructing families in the best manner to safely exit a burning building, and promoting the installation of smoke alarms and the purchase of fire escape ladders, a CSIRT may also perform a proactive role. This may include providing security awareness training, security consulting, configuration maintenance, and producing technical documents and advisories.

It has been the CERT/CC's experience that the first time many organizations start thinking about how to handle a computer security incident is after an intrusion has occurred. Why has your organization decided to start a CSIRT? Why has your organization decided to implement a CSIRT?

Benefits of a CSIRT

Reactive

- focused response effort
- more rapid, standardized, and coordinated response
- stable cadre of staff with incident handling expertise, combined with functional business knowledge
- collaboration with others in security community
- centralized point of incident response coordination and information dissemination

Proactive

- enables organizational business goals
- provides authentic risk data and business intelligence
- provides input into product development cycle or network operations
- assists in performing vulnerability assessments, developing security policies, and providing awareness training



Incident management is more than just implementing technology solutions it involves formalizing and standardizing a process for communication and coordination.

A CSIRT is different than a security team within an IT department.

A security team performs day-to-day monitoring of the network and systems of an organization. It is responsible for keeping systems up to date and installing patches, fixes, and workarounds to mitigate incident activity.

A CSIRT may perform these functions as part of their charter but also serve as a repository for incident information, a center for incident reporting and analysis, and a coordinator of incident response across an organization. This coordination can extend even outside the organization to include collaboration with other teams and law enforcement agencies.

What Does a CSIRT Do?

In general a CSIRT

- provides a single point of contact for reporting local problems
- identifies and analyzes what has happened including the impact and threat
- researches solutions and mitigation strategies
- shares response options, information, and lessons learned

A CSIRT's goal is to

- minimize and control the damage
- provide or assist with effective response and recovery
- help prevent future events from happening

No single team can be everything to everyone!



The goal of a CSIRT is to minimize and control the damage, provide effective response and recovery, and work to prevent future events from happening.

By definition, a CSIRT must perform at least incident handling activities. This entails analyzing, and resolving events and incidents that are reported by end users or are observed through proactive monitoring. This can mean determining the impact, scope, and nature of the event or incident, understanding the technical cause of the event or incident, identifying what else may have happened or other potential threats resulting from the event or incident, researching and recommending solutions and mitigation strategies, and coordinating and supporting the implementation of the response strategies. CSIRT staff require skills and expertise in understanding intruder attacks and mitigation strategies, the incident management processes, and how to respond to and coordinate the resolution of events and incidents.

Many organizations also assign the CSIRT responsibilities for more than the Respond process, such as protecting the infrastructure, detecting events and triage. It is up to each organization to determine which of the incident management capabilities its CSIRT will provide.

The goals of a CSIRT must be based on the business goals of the constituent or parent organizations. Protecting critical assets are key to the success of both an organization and its CSIRT.

Do you have any pre-conceived ideas or concepts about what a CSIRT does? Or what the various roles and responsibilities of a CSIRT could include? Is your definition of a CSIRT the same as your manager's or constituency's definition? If you are creating a CSIRT it will be important to set the right expectations with management for what the CSIRT can do and cannot do. You must ensure that you both have the same definition of functional responsibilities and corresponding authority.

Range of CSIRT Services

Reactive Services 	Proactive Services 	Security Quality Management Services 
<ul style="list-style-type: none">+ Alerts and Warnings+ Incident Handling<ul style="list-style-type: none">- Incident analysis- Incident response on site- Incident response support- Incident response coordination+ Vulnerability Handling<ul style="list-style-type: none">- Vulnerability analysis- Vulnerability response- Vulnerability response coordination+ Artifact Handling<ul style="list-style-type: none">- Artifact analysis- Artifact response- Artifact response coordination	<ul style="list-style-type: none">○ Announcements○ Technology Watch○ Security Audit or Assessments○ Configuration & Maintenance of Security Tools, Applications, & Infrastructures○ Development of Security Tools○ Intrusion Detection Services○ Security-Related Information Dissemination	<ul style="list-style-type: none">✓ Risk Analysis✓ Business Continuity & Disaster Recovery Planning✓ Security Consulting✓ Awareness Building✓ Education/Training✓ Product Evaluation or Certification

The CSIRT Development Team, in conjunction with the Trusted Introducer for European CSIRTs service, has updated and expanded the original list of CSIRT services presented in the original Handbook for CSIRTs (1998). This list is included in Appendix B of your tutorial materials. It is also available from the web at:

<http://www.cert.org/csirts/services.html>

According to this list, CSIRT services can be grouped into three categories:

Reactive services

These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, or something that was identified by an intrusion detection or network logging system. Reactive services are the core component of incident handling work.

Proactive services

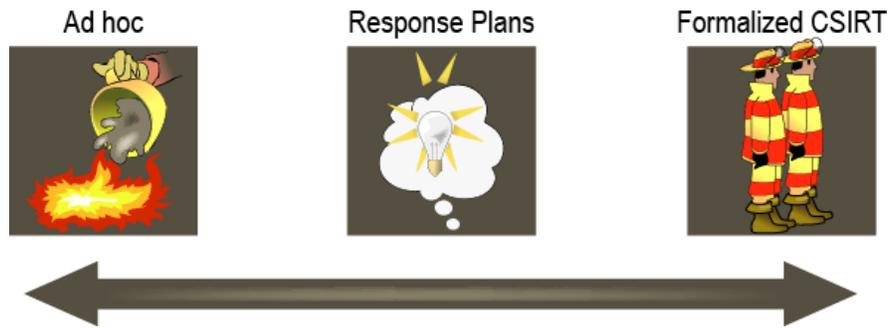
These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of future attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future. These services are ongoing, rather than being triggered by a direct event or request.

Security quality management services

These services augment existing and already well-established services that are independent of incident handling and traditionally have been performed by other areas of an organization such as the IT, audit, or training department. If the CSIRT performs or assists with these services, the CSIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive in nature but contribute indirectly, rather than directly, to a reduction in the number of incidents.

What is a CSIRT Capability?

Usually a CSIRT capability falls somewhere along the following continuum:



A CSIRT capability can take many forms. It can be an ad hoc or crisis team that is called together when an incident occurs. It can be a set of comprehensive policies and procedures for reporting, analyzing, and responding to computer security incidents. It can also be an established or designated group that is given the responsibility for handling computer security events and incidents. All of these different forms can generically be referred to as a CSIRT, a Computer Security Incident Response Team. So, in essence, the “team” is more of a capability, rather than always being a designated group of people who perform incident handling 100% of their daily work time.

These capabilities and teams can be configured in various organizational structures. Often we see the concept of extended teams, a core group performing daily CSIRT activities, supported, when necessary, by other experts throughout the organization or from external organizations. These people might have expertise in human resources, media relations, specific activities performed by organizational business units, audits, risk management, network operations or some other area. These types of staff members are often viewed as the “extended” team members of a CSIRT.

Evolving Nature of CSIRTs

There are many types of teams and capabilities, serving various constituencies.

These include teams in various sectors

- commercial
- government
- law enforcement
- military
- research and education
- critical infrastructure
- non-profit

Not all teams and capabilities

- have the same mission
- have the same authority
- perform the same role in the incident management process
- provide the same services



CSIRTs are not all structured in the same manner; they do not all perform the same function or even have the same name. Every CSIRT is different, and these differences may include the CSIRT's

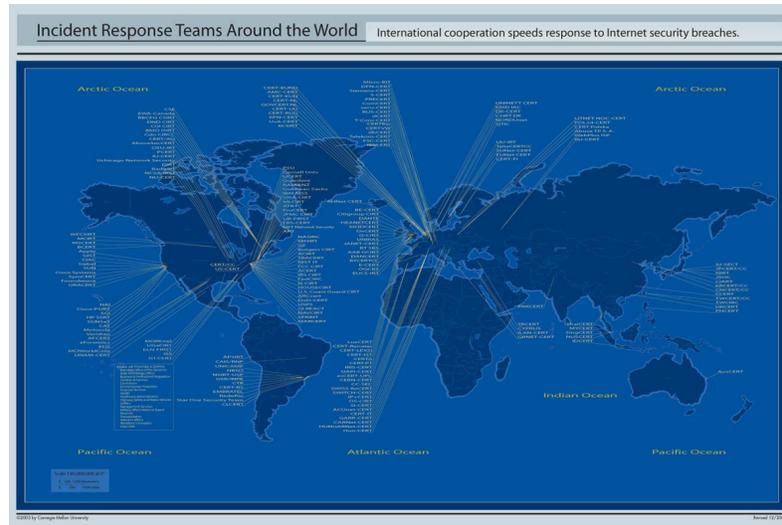
- mission, goals, and objectives
- constituency
- provided services
- definitions and terminology

We have presented a process model for incident management. Although the processes present a common approach to incident management, how each CSIRT implements those processes will be different. Each CSIRT is basically a different instantiation of those processes.

CSIRT Acronyms and Names

- CSIRT Computer Security Incident Response Team
- CSIRC Computer Security Incident Response Capability
- CIRC Computer Incident Response Capability
- CIRT Computer Incident Response Team
- IHT Incident Handling Team
- IRC Incident Response Center or Incident Response Capability
- IRT Incident Response Team
- SERT Security Emergency Response Team
- SIRT Security Incident Response Team

Variety of CSIRTs Across the Globe



CSIRTs come in all shapes and sizes and serve diverse constituencies. Some CSIRTs, such as the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), support an entire country. Other CSIRTs may provide support to a particular university such as Oxford, a commercial organization such as Boeing or SUN Microsystems, or a particular domain or IP range such as the Telia CERT Coordination Centre (TeliaCERTCC). There are also corporate teams and organizations that provide CSIRT services to clients for a fee, such as IBM Managed Security Services (IBM-MSS) or the debis Computer Emergency Response Team (dCERT).

General categories of CSIRTs include

- Internal or organizational CSIRTs - provide incident handling services to their parent organization; this could be a CSIRT for a bank, a university, or a federal agency.
- National CSIRTs – coordinate and facilitate the handling of incidents for a particular country, or economy. Usually will have a broader scope and a more diverse constituency.
- Analysis Centers – focus on synthesizing data from various sources to determine trends and patterns in incident activity. This information can then be used to help predict future activity or provide early warning when current activity matches a set of previously determined characteristics.
- Vendor Teams – coordinate with organizations who report and track vulnerabilities; another type of vendor team may provide internal incident handling services for their own organization.
- Incident Response Providers – provide incident handling services as a product to other organizations. These are sometimes referred to as Managed Security Service Providers (MSSPs).

Various global and regional organizations devoted to incident management collaboration and coordination have been created. This includes organizations such as the

- Forum of Incident Response and Security Teams
<http://www.first.org/>

National CSIRT Initiatives

Various countries have established national CSIRTs.

National CSIRTs have responsibility for a country or economy.

They can serve different constituencies

- government organizations
- critical infrastructures
- the public in general
- others

The goals of national initiatives can include

- establishing a focal point for incident coordination
- facilitating communications across diverse sectors
- developing trusted mechanisms for dissemination information
- promoting CSIRT and IM development and capacity building



The general role of a national team is to

- act as a trusted point of contact within the country and external to the country for
 - incident reporting
 - information sharing
 - incident response facilitation and coordination across sectors including vendors, ISPs, law enforcement, etc.
 - technical knowledge exchange
 - translation services
- perform outreach for incident response and security issues
- coordinate critical infrastructure protection initiatives
- promote CSIRT development and capacity building
- provide assistance in analyzing and responding to incidents and vulnerabilities
- provide trend analysis for incidents and vulnerabilities
- publish reports on incident trends and cybercrime within the country or economy

National teams are concerned with supporting the operational resiliency of their country. This would include

- defense systems
- critical infrastructures
- government systems

Related resources include

- CERT National Teams Page
<http://www.cert.org/csirts/national/>
- Steps for Creating a National Team
<http://www.cert.org/archive/pdf/NationalCSIRTs.pdf>

National CSIRT Examples

U.S. Computer Emergency Readiness Team (US-CERT)

<http://www.us-cert.gov/>

Australian Computer Emergency Response Team (AusCERT)

<http://www.auscert.org.au/>

Computer Emergency Response Team Brazil (CERT.br)

<http://www.cert.br/>

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

<http://www.jpccert.or.jp/>

Q-CERT, Qatar's Center for Information Security

<http://www.qcert.org/>



Software Engineering Institute | Carnegie Mellon

38

Here are a few examples of some National CSIRTs.

Regional Initiatives

Various areas have set up regional CSIRT initiatives.

- TF-CSIRT in Europe
- APCERT in the Asia Pacific area
- GCC-CERT in the middle east, Persian gulf area

These initiatives involve creating an organizational entity for participation by CSIRTs within a geographic area

These organizational entities

- are usually voluntary in nature
- can provide services or support to participating CSIRTs
- allow teams sharing similar legislative, cultural, and time zone issues to collaborate and coordinate incident handling activities



General role of a regional CSIRT organization

- provide an infrastructure for regional coordination of incidents
- assist with analysis and resolution of incidents and vulnerabilities
- provide forum for discussion and knowledge exchange
- provide a mechanism for collaboration to achieve economies of scale
- perform research and development in the area of incident management tools and best practices
- promote common standards and procedures for coordination
- provide input on addressing or understanding legal issues
- promote CSIRT development and capacity building

Regional initiatives include

- TF-CSIRT - Collaboration of Security Incident Response Teams in Europe
<http://www.terena.nl/activities/tf-csirt/>
- Asia Pacific Computer Emergency Response Team
<http://www.apcert.org/>



Creating an Effective CSIRT

  Software Engineering Institute | Carnegie Mellon 40

Elements of an Effective CSIRT

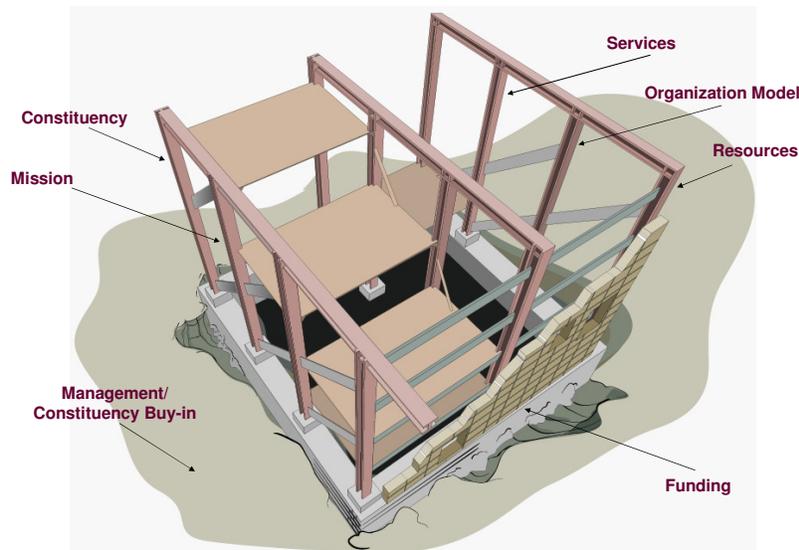


To be effective, a CSIRT requires four basic elements.

- operational framework
 - clear mission
 - defined constituency
 - organizational home
 - formal relationship to other organizational teams
- service and policy framework
 - defined services
 - defined information flow
 - defined process for collecting, recording, tracking, and archiving information
 - clear, comprehensive organization-wide policies
- effective quality assurance practices
 - definition of a quality system
 - specific measurements and checks of quality parameters
 - reporting and auditing practices and procedures
 - balance, compliance, and escalation procedures to ensure quality levels
 - constituency and customer feedback
- adaptability and flexibility
 - ability to adapt to real-time threats and future emerging threats
 - legal expertise and support

These elements help to define the basic requirements and benchmarks against which a CSIRT can evaluate its operation and effectiveness.

Building Your Vision



The basic components or building blocks of your CSIRT framework make up your CSIRT vision. These components include:

- Constituency - Whom do you serve?
- Mission - What do you do? What is your purpose?
- Services - How do you accomplish your mission. How do you service your constituents?
 - What type of incidents do you handle?
 - What type of activities do you perform?
- Organizational Structure - How do you operate? How is it tied together?
- Resources - What resources do you need to perform your mission?
- Funding - How do you pay for it? All of the above is supported by funding.
- Management and constituent buy-in - without this it won't succeed. This is the ground that the vision stands upon.

The components of a CSIRT influence each other and therefore influence your design. For example, your mission will be influenced by your constituency and needs. Your resources and how they are dispersed will influence the organizational model you need, the services you will be able to provide, and how well you can execute your mission.

In defining your vision or framework, you must take all of these components into consideration while finding the right balance between them.

General Implementation Recommendations

Get management buy-in and organizational consensus.

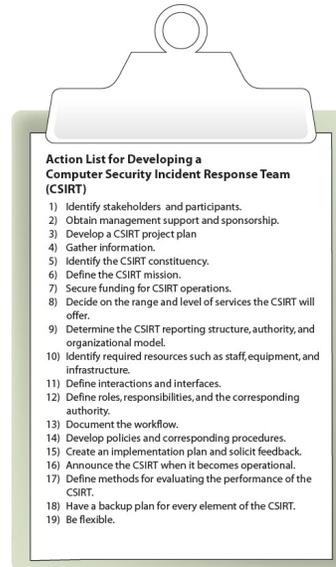
Match goals to parent or constituent organizational policies and business goals.

Select a CSIRT development project team.

Communicate throughout the process.

Start small and grow.

Use what exists, if appropriate. (Reuse is good.)



A CSIRT planning team project leader with authority for decision making should be established. The project team should be representative of involved parties and groups.

All stakeholders and constituency representatives should be involved in the development of the CSIRT from the initial planning stages through the implementation.

In a commercial or educational organization, this may include legal advisors, public relations and marketing staff, departmental managers, security staff, system and network administrators, helpdesk staff, upper-level management, and perhaps even facilities staff.

It is harder to determine who the stakeholders are and when a coordination center or national team is being established. Some of this may be able to be determined once you choose or define the constituency to be served.

Getting involvement early on can work as an initial marketing effort for your CSIRT, it begins to build awareness.

Management buy-in must include providing personnel, time, and funding.

A CSIRT's structure and mission must build on the parent or constituent's organizational security policies and business goals.

Make sure that everyone understands what is happening and why it is happening throughout the process.

Where possible, use existing resources and security policies and strategies. For example, if there is a physical security breach at your organization - who is currently notified? What process is followed? Can you use this existing policy to create a policy for an electronic breach? Can the old policy cover both types of breaches?

Build on what already exists, both internally and externally. Talk with other teams to find out what has worked well for them. It may also work for you depending on your structure and mission.

Action Plan -1

Identify stakeholders and participants

Obtain management support and sponsorship

Develop a CSIRT project plan

Gather Information



Source: *Action List for Developing a Computer Security Incident Response Team (CSIRT)*
http://www.cert.org/csirts/action_list.html

Different stakeholders may be needed for each phase of CSIRT development, implementation and operation.

- Common problems: The right stakeholders and participants are not identified and included in these phases; other stakeholders, participants, and business managers are not aware that a CSIRT is being planned.

Executive management and sponsorship for development and acceptance of CSIRT is critical

- Common problems: support from leadership and strategic partners is not obtained and CSIRT planning suffers

Form a project team to help with the development of the CSIRT, assign roles and responsibilities for this team

- Common problems: the project team does not involve a diverse set of stakeholders; a reasonable timeframe is not established for the project's completion, a project leader is not established and the project languishes without direction or completion.

Ask questions about constituent's needs, types of activity, incidents, and problems that are occurring and approaches to handle. Determine the different legal, political, business, technical or cultural issues that will affect CSIRT operations.

- Common problems: the rights sets of input are not obtained; there are disagreements over who owns the data and intellectual property which can cause delays in providing CSIRT information to the constituency.

Action Plan -2

Gather information (cont.)

Key information to gather includes

- What needs does the constituency have?
- What are the critical assets that must be protected?
- What types of incidents are frequently reported?
- What computer security problems exist?
- What type of response is needed?
- What assistance and expertise is needed?
- What processes are required?
- Who will perform what role?
- Is anyone currently performing that role?
- Who needs to be involved in the notification or escalation processes?

Available resources that may provide information

- organization charts for the enterprise and specific business functions
- topologies for organizational or constituency systems and networks
- critical system and asset inventories
- existing disaster recovery or business continuity plans
- existing guidelines for notifying the organization of a physical security breach
- any existing incident response plans
- any parental or institutional regulations
- organizational information classification schemes



Many of the resources listed here may not be available or may not exist within your organization. If they do and you can obtain access to them, reviewing these documents can serve a dual purpose: first, to help you identify existing stakeholders, resources, and system owners; and second to provide an overview of existing policies to which the CSIRT must adhere.

As a bonus, you may find that these documents may contain text that can be adapted when developing CSIRT policies, procedures, or documentation. They may also include general notification lists of organizational representatives who must be contacted during emergencies – these types of lists may also be able to be adapted for CSIRT work and processes.

Action Plan -3

Identify the CSIRT constituency

Define the CSIRT mission

Secure funding for CSIRT operations

Determine the range and level of services to be offered

Determine the CSIRT

- reporting structure
- authority
- organizational model



Determine initial set of 'customers' (stakeholders, sponsors, partners, constituent members, business owners/operators, etc.), as well as longer-term constituent members.

- Common problems: not all constituents are addressed or defined--leads to lack of formal interface with the CSIRT. CSIRT products not effectively marketed to show benefits to the constituency. Unclear guidelines for contacting the CSIRT. CSIRT tries to support too many diverse constituencies during its startup.

Design mission statement to define the purpose and function of the CSIRT. It should be broadly framed to remain relevant if (or when) CSIRT services change. Determine primary goals and objectives when defining the CSIRT mission.

- Common problems: staff don't understand the mission. Loss of mission focus. External influences (e.g. political) can try to pull the team into activities it is not prepared to handle.

Identify funding for short-term start-up operations as well as long term sustainment and growth of the CSIRT

- Common problems: Inadequate funds to hire people needed for services provided. No training funds to keep knowledge, skills, abilities current with CSIRT or constituency needs. The CSIRT can become less able to handle new threats, attacks, and risks that affect their constituency over the long term.

Define service levels and who has access to what services

- Common problems: Constituents want services before CSIRT is ready to provide. CSIRT tries to offer too many services at once. CSIRT takes on too many roles or creates unneeded services.

Establish where CSIRT resides (is it in a larger organizational structure, a government office or ministry, an external service provider, etc.). Create organizational chart. Identify reporting requirements/regulations.

- Common problems: non-CSIRT assignments are imposed by outside stakeholders that pull CSIRT staff away from their primary CSIRT functions.

Action Plan -4

Identify required resources

- staff
- equipment
- Infrastructure

Define CSIRT interactions and interfaces

Define roles, responsibilities

Document the workflow

Develop policies and procedures



Define resources needed and processes for CSIRT work. Identify knowledge, skills, and abilities (KSAs) needed. Determine training needs.

- Common problems: staff is not cross-trained. 'Single points of failure' can result. No training or professional development plans for long-term sustainment and growth. No contingency planning for staff terminations or reassignments.

Identify the interactions between stakeholders and CSIRT. Determine who owns data and has authority over it. Establish how, and with whom, data is shared, protected, controlled, stored, accessed, destroyed, etc.

- Common problems: If not properly done, information can be disclosed inappropriately. CSIRT staff is not informed about CSIRT activities, reducing effectiveness in normal work roles. Defined interfaces are not established, causing a process breakdown when escalation or data sharing and coordination is required. Can affect reputation.

All CSIRT functions should be defined with assigned roles and responsibilities. The interfaces between these roles and functions should be clearly understood to avoid confusion, overlapping roles, or gaps.

- Common problems: More than one group is given the same responsibility. Staff unclear on what their role is, where it ends and someone else's role begins. No specific responsibility is assigned and the task is never completed.

Establish clearly how work flows within the CSIRT to identify all the processes. Identify quality assurance checks and balances.

- Common problems: Staff not aware or don't follow correct processes. Service delivery may be insufficient or missing. Interactions with correct stakeholders may fail.

Identify the needed policies, procedures, guidelines, checklists to ensure staff perform their responsibilities effectively. Identify appropriate guidance for incident categorization, prioritization, escalation criteria

- Common problems: common definitions are not shared between the CSIRT and constituency. Unable to summarize data on incident trends because there is no clear definition of terms. Lack of formalized policies delay response time (processes are not consistent, repeatable, reliable)

Action Plan -5

- Create an implementation plan and solicit feedback
- Announce the CSIRT when it becomes operational
- Define methods for evaluating the performance of the CSIRT
- Have a backup plan for all elements of the CSIRT
- Be flexible and adaptable



Have a structured plan for implementing the CSIRT with a timeline and milestones. Make sure the plan is seen by relevant stakeholders and members of the constituency.

- Common problems: the constituency is not informed about the CSIRT implementation and does not provide support, which may result in incidents not being reported to the CSIRT or CSIRT advice and recommendations not being followed; the implementation plan is not sent for review, resulting in a plan that is not supported or implemented. Common problems: the CSIRT is not formally announced, and no one understands how or when to interface with the team.

Determine baselines for CSIRT benchmarking of basic processes and functions. Choose methods to assess if the CSIRT is meeting its mission and the requirements of the constituency.

- Common problems: no methods are instituted for evaluating whether the CSIRT is accomplishing its mission; methods for process improvement are not implemented; performance metrics do not adequately measure CSIRT performance

Have a tested plan in place for providing services if resources, equipment, or infrastructure is lost.

- Common problems: the CSIRT has no surge capacity if additional staffing is needed during peak or emergency situations; key CSIRT systems and networks that provide critical functions and services are not backed-up, resulting in the CSIRT not being able to function during an emergency situation.

Learning from Others

Review existing CSIRTs' Web pages, look at their defined

- constituency
- mission
- services
- funding strategies

Talk to other CSIRT staff members

- conferences such as FIRST
- site visits

Read existing documents and guidelines



As you begin to establish your vision and framework – look to other teams, existing documents and books on incident response as a source for helpful resources and ideas.

Investigate what similar organizations are doing to provide incident handling services or to organize a CSIRT. If you have contacts at these organizations, see if you can talk to them about how their team was formed. If you cannot talk with team members, take a look at other CSIRTs web sites. Check their missions, charters, funding scheme, and service listing. This may give you ideas for organizing your team. Review any books and any white papers people may have written about Incident Handling or CSIRTs. An initial list of resources can be found at the CERT CSIRT Development Web page:

<http://www.cert.org/csirts/resources.html>

Building a CSIRT - Where To Begin?

What's already in place – create a matrix of expertise.

- What expertise exists?
- What processes are already in place?
- What tools and infrastructures are already in place?

Brainstorm and discuss – design the workflow.

- What is the desired response and notification strategy?
- What needs to be changed with the addition of a CSIRT?
- How does the CSIRT fit into any disaster recovery or business continuity plans?

Implementation – build staff and processes.

- Develop the interim plan.
- Develop the long-term plan.



It is important to understand the roles and functions being performed by the CSIRT and to identify who else is involved.

This may include management, other technical and legal or investigative personnel. Defining the interfaces between groups and establishing a standard and consistent process for these groups to work together will make or break your incident management capability.

Identifying areas of expertise, defining roles and responsibilities, and outlining rules of engagement for any interface between groups are key steps to begin building an effective capability.

Other questions to ask include

- Will you need to integrate your tracking system with any existing trouble ticket databases?
- Will you need to comply with any specific organizational requirements and policies?
- Are there service level agreements you must meet?

Strategies for Building or Improving Your Capability

Document your current incident management processes.

- define your **As-Is** or current state of incident management processes
- perform a gap analyses of the current state against a chosen benchmark.

And then

- develop the **To-Be** or future state of your incident management or CSIRT processes
- define staff, processes, procedures, policies, training, etc. needed to fill gaps and reach the To-Be state



You can use the Incident Management Process Model and Framework as a benchmark to define the components for these areas

- Prepare/Sustain/Evaluate
- Protect Infrastructure
- Detect Incidents
- Triage Incidents
- Respond

You can also use as benchmarks

- Resiliency Engineering Framework Incident Management and Control (REF IMC) capability
- Incident Management Capability Metrics
- ISO 27002 (*Information technology - Security techniques - Code of practice for information security management*) and related ISOs
- Information Technology Infrastructure Library (ITIL)
- Other organizational benchmarks

Documenting the As-Is State

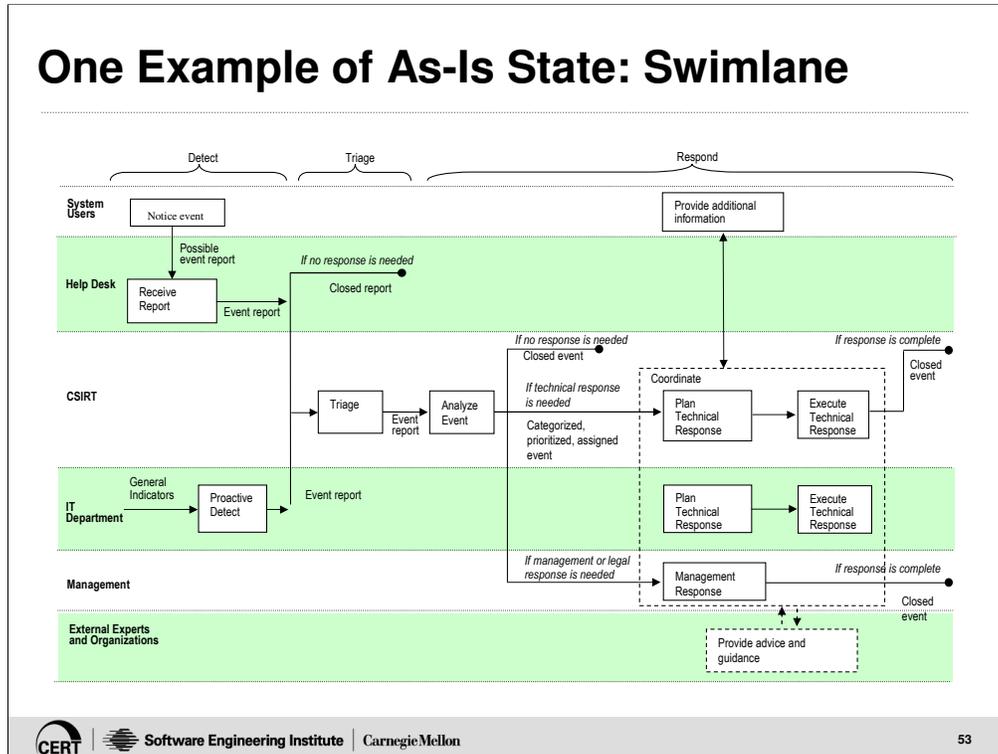
Document the current

- processes and corresponding workflows in place to handle incidents
- organizational staff or units involved in receiving and handling incidents
- policies and procedures that govern incident handling in the organization

If using the IM Process Model build the As-Is process map using the general model

- redline or modify the generic process map
- add any relevant new processes, activities, or interfaces
- revise process descriptions for each process, activity, and interface
- review and finalize

One Example of As-Is State: Swimlane



Here is an example of a Swimlane Diagram.

The process workflow diagrams and descriptions in the model are very generic in nature. An organization customizes the document for their own situation, and begins to add the roles and responsibilities associated with each process.

- Using this organization-specific information, the process workflow for an organization will look different from our generic workflows.
- It will show the workflow or routes of the work and who is responsible for performing the work.

See Appendix H for a larger version of this slide.

Gap Analysis

Perform a traditional process gap analysis by looking for characteristics such as

- missing activities or services
- missing or poorly defined handoffs
- missing or poorly defined aspects of each process activity (e.g., no procedures or inadequate staff)
- bottlenecks in the process
- poorly defined activity flows (e.g., too much parallelism, too linear, too many handoffs)
- single points of failure
- duplicate work activities

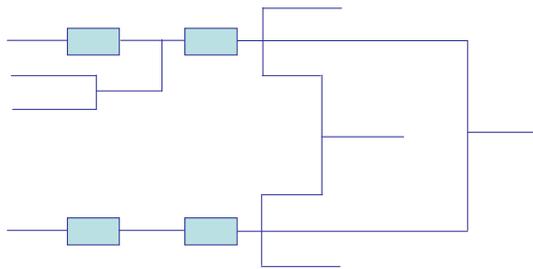


Once you have defined how you are currently performing incident management tasks, compare them to your chosen benchmark and note where there are differences.

Building the To-Be

Build the To-Be process map by modifying the As-Is

- identify new activities
- identify improvements to poor characteristics such as missing procedures or poorly trained staff
- streamline inefficient flows
- eliminate bottlenecks through process redesign
- remove duplicate or ambiguous activities



Once you have identified the gaps, prioritize the improvements you will make based on

- resources
- funding
- time
- need
- feasibility

Complete the To-Be Process

Use the To-Be process as the goal for improvement planning

- prioritize and schedule changes, such as
 - adding additional activities or services
 - building missing procedures
 - acquiring needed training
 - adding personnel
 - revising contracts for improved handoffs
 - defining new interfaces and communication channels
 - update service or outsourced contracts with new process needs
- monitor progress and watch for unintended consequences (e.g., unexpected bottlenecks)
- re-evaluate the revised process



Based on your To-Be state, build a process improvement implementation plan.

Document Your Vision

Define your vision in a Concept of Operations Document.

Clearly articulate your

- constituency
- mission
- organizational home
- authority
- set of services
- organizational model
- defined relationships and interfaces (internal and external: such as IT, legal, law enforcement, human resources, etc.)
- work processes through workflow diagrams, descriptions of roles and responsibilities
- governing list of policies and procedures
- event and incident reporting guidelines (criteria, categories, priorities, escalation criteria, etc.)
- CSIRT or IMC contact information



Document your vision for a new team or for any improvements you plan to make.

As appropriate, the Concept of Operations may also include business planning materials (financial and budgetary guidance), continuity of operations, disaster recovery, or other relevant documents either by explicit inclusion or by references to other existing documentation.

Common Problems

Failure to

- include all involved parties
- achieve consensus
- develop an overall vision and framework
- outline and document policies and procedures



Organizational battles

Taking on too many services

Unrealistic expectations or perceptions

Lack of time, staff, and funding



Constraints can include

- budget ceilings or lack of funding
- geographic dispersion of organization
- organizational disagreements or factions
- lack of management understanding and buy-in
- lack of experienced personnel resources
- lack of a clear vision, consensus, or expectation across the organization
- lack of communication
- impractical timeframes

Some constraints may never be able to be overcome. However, methods for dealing with problems and factions may include

- ensuring everyone has a clear vision of what is happening
- ensuring that all opinions are asked for and taken into account
- building a project team with a wide representation
- meeting with factions to talk in person
- getting various groups together to work as a team in the planning and design phases
- ensuring everyone knows their role
- obtaining management support for CSIRT
- providing security awareness training
- providing copies of reporting guidelines to all constituents and organizational entities

When dealing with budget and resource constraints, solutions may include:

- limiting the mission and services of your CSIRT
- training and utilizing existing staff
- collaborating with other CSIRTs to use their services and expertise

It All Depends

A successful implementation will depend on

- developing a vision with input from the rest of the organization
- the clarity of that vision
- the support of that vision
- obtaining available resources including staff, expertise, and funding
- communicating your vision and strategy
- building a reputation of trustworthiness for your team

This may be affected by unique constraints within your organization.



Recognize that the “business climate” or “environment” will impact the organizational framework—not only for how effective your CSIRT will be, but also what services you may be able to provide and the level of support for each service.

Novice vs. Mature Teams

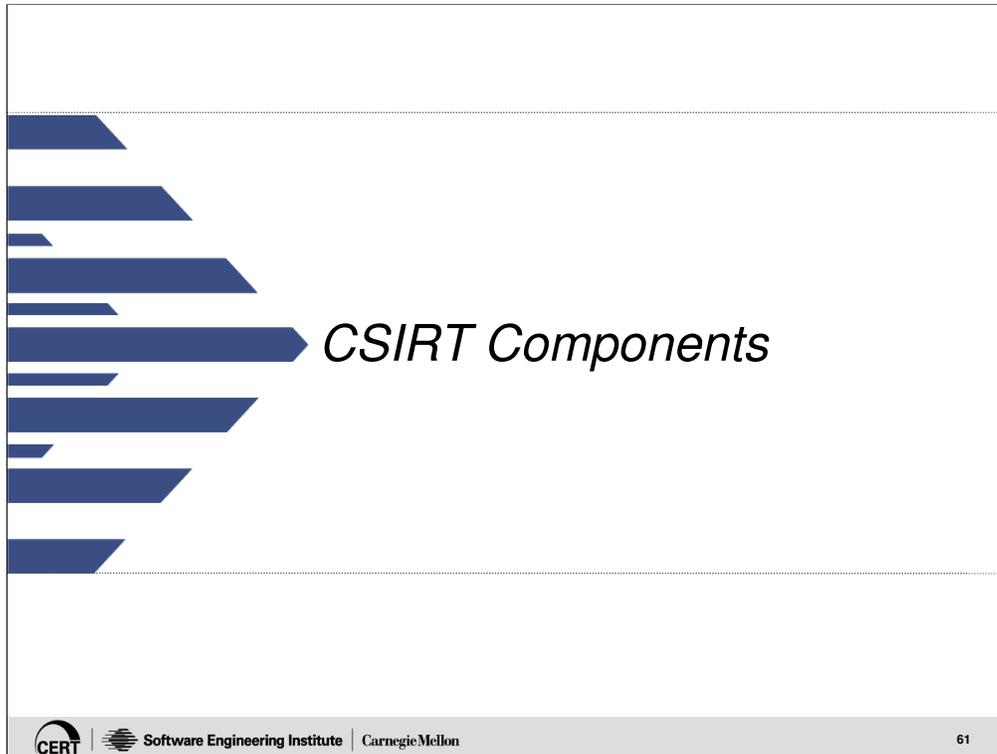
CERT experiences have shown that generally new teams

- need time to establish relationships with constituents, stakeholders, and collaborators
- end up focusing on more reactive versus proactive services
- have less well defined interfaces and procedures

While more mature teams generally

- have documented processes, policies, and procedures
- have well defined interfaces and communication channels
- have instituted and enforced a training and mentoring plan
- have a quality assurance program in place
- have an evaluation mechanism in place to measure their success
- participate in more collaboration and data sharing activities
- balance between reactive and proactive services
- provide input into quality management services





CSIRT Components

- Constituency
- Mission
- Funding
- Organizational Issues
- Services
- Policies and Procedures
- Resources

Identify Your Constituency

Defining your constituency will help scope your work and refine your mission.

- Your constituency may already be defined for you depending on your organization.
- If not, you will need to determine who or what it will be.

Your constituency may evolve over time as new needs or requirements are determined.



Understanding your constituency will help you to determine what needs they have, what assets need to be protected, and what the requirements for your CSIRT will be. Using this information will help you determine what services you have to offer and what organizational model will fit the needed service delivery.

Defining your constituency will also help you scope your work when your team becomes operational. It will help determine what requests you will handle and what requests you will pass on to other CSIRTs or other relevant parties.

As you get started, you may find that you need to define a short-term and long-term constituency. There maybe a group that you work with initially, and then later expand your services to a broader constituency.

Some teams may have their constituency already defined. For example, a CSIRT in a small commercial business will most probably have the employees of that business as their constituency. However, it may not be so easy to define a constituency. A CSIRT at a university could have as its constituency the systems and networks administrators in the various departments or the entire university population including all faculty and students. This distinction is important. For a university CSIRT it will determine at what level alerts and advisories are written and what type of response is made.

As mentioned before, determining the constituency for a national or state team, or for a coordination center can be difficult. But this must be done as it will affect who needs to be involved in the planning process and what type of services will need to be provided. The question must be asked – with whom will the coordination center or national team work and collaborate. To whom will they send out notifications, alerts, and other information? Options might include other government agencies, critical infrastructure organizations, military agencies, or the general public. Each constituency will have its own needs and requirements.

Identify Strategic Partners

In identifying your constituency think about who you will work with and provide service to in both the short and long term.

Strategic partners may be the first part of the constituency to whom you provide service or with whom you work.

You may provide a special level of service to strategic partners.

Strategic partners can also work with you to help communicate your CSIRTs message.



To be successful, a CSIRT must have an impact far greater than its dedicated technical staff can achieve alone.

- It is critical that teams cultivate relationships with individuals and organizations at all levels to help communicate its message.
- This includes both internal and external partners.
- One way to do this is through the establishment of relationships with strategic partners.

Strategic partners can be especially critical for developing National CSIRTs.

Government ministries, corporations, academic institutions, vendors, other incident response teams, and home users all play an important part in improving internet security and can be effective partners.

Strategic partners can

- help guide the priorities and direction of the CSIRT, and help define and mature the CSIRT's capabilities and services
- engage in information sharing and research activities
- participate in customized interactions with the CSIRT.
- help to increase the visibility and influence of the team
- help promote the adoption and use of best security practices throughout the constituency
- help build capabilities within other organizations

Determine Your Mission

Your mission should be defined in your CSIRT Mission Statement (and included in your Concept of Operations, as well as other appropriate documents).

RFC 2350 states that your mission should :

- explain the purpose of your team
- highlight the core objectives and goals of the team



RFC 2350, Expectations for Computer Security Incident Response, is a best practices document that provides information on general topics and issues that need to be clearly defined and articulated to a CSIRT constituency and the general Internet community. [RFC2350, Abstract]

Some CSIRTs develop a broader statement in the form of a charter which outlines their mission, constituency, sponsor, and authority. [RFC2350, section 3.3]

According to the CSIRT Handbook (page 10-11) your mission statement should:

- “be non-ambiguous”
- “consist of at least three or four sentences specifying the mission with which the CSIRT is charged”
- “if the team is housed within a larger organization or is funded from an external body, the CSIRT mission statement must complement the missions of those organizations”

Issues to be addressed may include:

- How to obtain management support for the defined mission?
- How do you deal with the public perception of CSIRTs as “cybercops”?
- Will the CSIRT perform repair and recovery operations or provide support only?
- What is the basic goal of the response process – recover and repair systems or track and trace?
- Will intruder compromises and activity require prosecution? This can set one of the service requirements – will forensic evidence collection services be required and if so will the CSIRT perform this function?
- Who will control perimeter and internal defenses? Will the CSIRT be responsible for IDS or firewalls?

Obtain Funding for Your CSIRT

Various strategies exist for funding your CSIRT:

- membership subscription
- fee-based services
- contract services
- government sponsorship
- academic or research sponsorship
- parent organization funding
- consortium sponsorship
- a combination of the above



Membership subscription

- time-based subscription fees for delivery of a range of services
- AusCERT has a membership subscription

Fee-based services

- adhoc payment for services as delivered
- AusCERT has a fee-based SMS alert service, MYCERT at one time had special fee-based services

Contract services

- outsource CSIRT to organization providing incident handling service
- commercial groups such as IBM, ISS, CISCO, and other consulting firms

Government sponsorship

- government funds the CSIRT
- US-CERT is sponsored by the U.S. government

Academic or research sponsorship

- university or research network funds the CSIRT
- SURFcert and NORDUnet CERT are both sponsored by research networks

Parent organization funding

- parent organization establishes and funds CSIRT
- IBM, Cisco PSIRT, etc. are members of FIRST

Consortium sponsorship

- group or organizations, government entities, universities, etc. pool funding

Combination of the above

- CERT/CC is funded by government and private sponsorship

Define Your Range of Services

The range and levels of services provided by teams will depend on a number of factors.

Each team must determine what

- range of services is appropriate for their constituency
- level of support will be provided for those services



Not all CSIRTs provide the same set of services. This slide lists some common services that a team could provide. Definitions for these services can be found in Appendix B.

For a team to be considered a CSIRT, it must provide an incident handling service. That means it must provide at least one of the incident handling activities: incident analysis, incident response on site, incident response support, or incident response coordination.

To learn more about various services offered by different CSIRTs you can

- talk with existing teams
- review team web pages and lists of services
- review general incident handling service lists

Example Base Set of CSIRT Services

Reactive Services

- alerts and warnings
- incident handling
 - incident analysis
 - and at least one of the following: incident response resolution, incident response support, incident response coordination
- vulnerability handling
 - vulnerability response coordination

Proactive Services

- announcements
- technology watch

Security Quality Management Services

- awareness building
- security consulting – particularly developing security policies



Although we mentioned that to be a CSIRT a team needs to provide (at a minimum) an incident handling service, in reality, according to the CERT CSIRT Development Team, most new teams forming provide much more. As a result, a baseline set of services has emerged that appears to be appropriate for initial consideration by any CSIRT. This baseline set of services has been developed by the CERT CSIRT Development Team from resources such as the Handbook for CSIRTs, the collective knowledge and experience in incident response activities gained over the last decade by CERT/CC and many other teams, discussions with other CSIRTs, and a review of available literature.

Note: Announcements as listed above only refers to accepting information about vulnerabilities and passing that information along to another group or team for further investigation, response, analysis, and other support. It is a very basic handling of the information to facilitate dissemination to the appropriate individuals.

National CSIRT Common Services

Reactive Services

- alerts and warnings
- incident handling
 - incident analysis
 - incident response coordination

Proactive Services

- technology watch
- security related information dissemination
- vulnerability response coordination

Security Quality Management Services

- awareness building
- security consulting – particularly developing security policies
- training – capacity building



This slide provides a sample list of services that a national team may provide. It is not an exhaustive list, nor meant to be restrictive to just this set. Rather it provides suggestions that a national team might want to consider.

Many National teams provide “point of contact” activities to help report and coordinate incidents.

They can also act as liaisons between affected sites and government organizations, law enforcement, or other security groups.

When Selecting Services

Make sure you are providing services that the constituency really needs.

Think about this for the short and long term

- define your initial set of services
- have a plan for services you want to offer in the long-term

Start small and grow

- gain support for the initial services
- grow as expertise and funding is available



Some CSIRTs provide a full set of services including incident handling, vulnerability handling, intrusion detection, risk assessments, security consulting, and penetration testing. Other CSIRTs provide only a limited range of services. For example, a few military organizations provide only intrusion detection services while some government organizations provide only a referral service, referring incidents to third-party contractors such as the US-CERT or the CERT Coordination Center (CERT/CC).

It is recommended that a CSIRT start with a small subset of services, gain acceptance of the CSIRT by the organization through quality service and response, then begin to develop and expand the capabilities of the CSIRT as they are needed and can be effectively supported.

Define Your Organizational Model

What model will best serve your constituency?

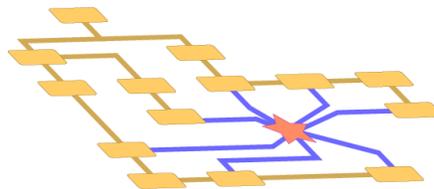
How will the CSIRT operate and interact with your organization and constituency?

Models include

- Security Team
- Internal Distributed Team
- Internal Centralized Team
- Combined Distributed and Centralized Team
- Coordinating CSIRT

You may need more than one model.

Your model may evolve over time.



This model should take into account:

- interactions that must take place
- information flows
- internal staff and external parties to be involved
- location of CSIRT staff
- requirements and needs of the constituent or organizational sites
- infrastructure for these interactions

Organizational Decisions

Initial organizational decisions

- Will the CSIRT be part of an existing organization or will it be a stand-alone organization?
- Where will the CSIRT be located?
- What authority will the CSIRT have?
- How will the CSIRT be operationally structured?
- How will information be shared throughout the organization or constituency?

Other issues to be determined

- operating hours of the CSIRT
- staffing
 - full time staff or part-time
 - shift coverage
- in-house or outsourced technical support
- available “reach back” capability



How will the CSIRT operate and interact with your organization and constituency?

- What type of operational hours will the CSIRT have:
 - business hours only
 - 24x7
 - full staff for business hours, and on call for after-hours
- If your CSIRT will provide support beyond the typical 8-hour day, what type of shift coverage will be needed:
 - three 8 hour shifts
 - two 12 hour shifts
- Will there be dedicated CSIRT staff or will you pull in staff from other parts of the organization
 - ad hoc staff may come together when there is an incident
 - could also have core staff and pull in subject matter experts as needed
- If part of the CSIRT or incident management capability is to be out-sourced
 - What parts will be outsourced?
 - How will compliance, governance, and information sharing issues be handled?
 - What type of service level agreements will be put in place?
- What type of reach back capability will be in place?
 - Can you call on other parts of the organization as backups, such as IT staff, if additional assistance is required?
 - If you have contracted staff, can the contractor pull more staff to help in peak times?

Reporting Structure: Internal CSIRT

Some questions to be asked

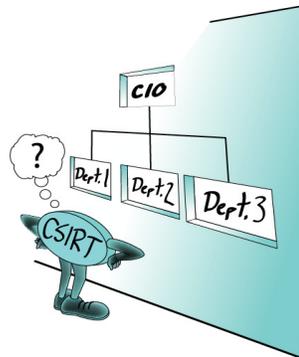
- Where does the CSIRT fit in the organization?
- To whom does the CSIRT report?

This will depend often on what part of the organization has responsibility for security issues.

For example it could be under the

- CSO
- CISO
- CRO

It should be higher up in the organization, where it can obtain enterprise-wide collaboration.



The two questions asked above are dependent on one another. To whom the CSIRT reports will depend on where it is located in the organization and vice versa.

In today's organizational structures, the CSIRT would not normally be part of the IT department, but be outside that area, in an independent capacity. This may mean that they report to the

- Chief Security Officer (CSO) – if this is where cyber security issues are handled
- Chief Information Security Officer (CISO) – if physical and cyber security are combined
- Chief Risk Officer (CRO) – if the risk management area has incorporated security risks into its domain

The CSIRT could be an independent unit reporting to a specific Business Manager.

Wherever it is located, it should be at a level where it can get agency wide collaboration and information sharing, and enforce when necessary its mandate. It is important to think about what actions the CSIRT will need to take and what type of management support will be required to facilitate those actions during incident handling and response. Identifying such issues may suggest the right reporting or management structure.

Any specific contractual or legal obligation may impact this reporting structure. For example, the CSIRT may be contracted to support a specific constituency or organization. This contract may require specific decisions makers to be involved in CSIRT actions or for specific information to be reported on a periodic basis. Your management may also require periodic updates of CSIRT activity or department heads and other managers may want to be involved in CSIRT response decisions. For example, the CERT/CC must obtain approval from its sponsors for various actions it may take or agreements it may enter into.

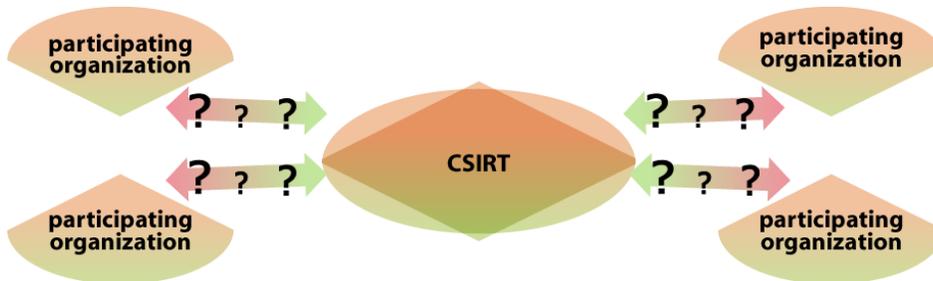
As you plan your team, it will be critical to decide how the CSIRT will

- interact with any information technology department
- fit into the change management and software installation and upgrade processes
- work with the investigative or law enforcement group
- make recommendations for changes to internal and external defenses like firewalls or IDS

Reporting Structure: National Team

Some questions to be asked

- Who will host the CSIRT?
- Where will the CSIRT be physically located?
- Who owns the intellectual property that is produced by the CSIRT?
- Will the constituency be broad or a small selective group?



For teams that serve as a coordination center or support a state, national, provincial or similar government entity constituency – it is even more difficult to determine how the relationships with the participating organizations should be structured

Will the CSIRT only deal with particular organizations such as

- Government organizations
- Military organizations
- Critical infrastructures
- Business organizations

Will the CSIRT accept reports from and disseminate information to the public?

CSIRT Authority

What is the authority of the CSIRT?

- Full
- Shared
- No Authority

Or is it something else?

- Indirect Authority
- Other?



Authority describes the control that the CSIRT has over its own actions and the actions of its constituents, related to computer security and incident response. Authority is the basic relationship the CSIRT has to the organization it serves. Authority goes hand and hand with the location of the CSIRT in any organization.

According to the Handbook for CSIRTs (page 15), there are three distinct levels of authority or relationships that a CSIRT can have with its constituency:

- Full - The CSIRT can make decisions, without management approval, to implement response and recovery actions. For example: A CSIRT with full authority would be able to tell a system administrator to disconnect a system from the network during an intruder attack or the CSIRT, itself, could disconnect the system.
- Shared - The CSIRT participates in the decision process regarding what actions to take during a computer security incident, but can only influence, not make, the decision.
- No Authority - The CSIRT cannot make any decisions or take any actions on its own. The CSIRT can only act as an advisor to an organization, providing suggestion, mitigation strategies or recommendations. The CSIRT can not enforce any actions. The CERT/CC is a CSIRT that has no authority over its constituency, which is the Internet community.

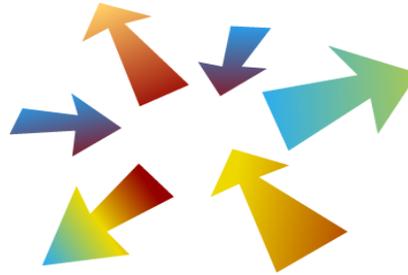
Another type of authority highlighted on page 15 is “Indirect Authority”. In this case, the CSIRT due to its position may be able to exert pressure on the constituent to take a specific action. An ISP for example may be able to force its constituents to take a specific action or face discontinuation of Internet services.

For a CSIRT to be successful in its mission, it is critical that management approves and supports the level of authority that the team will have, otherwise, the team will lose credibility within the organization and will not be successful. Management should also adequately and clearly convey the CSIRT authority to the constituency—particularly division managers, system and network administrators, and any other groups within the organization.

Collaboration and Coordination

Who else do you have to work or share data with?

- other security experts
- other CSIRTs or coordination centers
- law enforcement
- other government agencies
- constituency Internet Service Provider (ISP)
- other groups in your organizations
 - IT department
 - public relations
 - human resources
 - legal department
 - security groups



When defining your information flows and processes, think about who else you may need to communicate with or involve.

This may provide opportunities for collaboration, research, or obtaining assistance.

What preparation can be done beforehand?

- obtaining and storing contact information
- obtaining and validating PGP keys or digital certificates for information exchange
- installing and testing secure phone lines

What expectations do they have for the interaction?

- provide advice
- simple FYI notification
- actually collaborate on solutions and analysis

If you are a local corporate CSIRT you may need to have access to network and system logs and configurations such as

- firewall logs and rules
- mail server logs
- IDS logs
- network or host connection monitoring logs

If your CSIRT does not maintain these logs, what relationships need to be established to get access to this information? And at the next level, what if new configurations, signatures, or filters need to be installed at the network level or on applications? Does your CSIRT have in place a process to get these recommendations implemented in a quick and easy manner?

If you are a coordination center who will you need to help you do the analysis? What type of information will you need to do the analysis, if your team does this at all. You may need to work with another set of security experts who will actually perform the analysis. Of course any non-disclosure agreements must be in place before you can involve others in your analysis.

Develop CSIRT Policies and Procedures

All services and CSIRT functions should be supported by well-defined policies and procedures.

Documented policies and procedures are vital to

- ensure team activities support the CSIRT mission
- set expectations for confidentiality
- provide the framework for day-to-day operational needs
- maintain consistency and reliability of service

These also provide guidance or support for

- roles and responsibilities
- priorities and escalation criteria
- appropriate responses
- new CSIRT staff members
- compliance with regulatory requirements

Start with the most important and needed policies and procedures.



When possible, correlate the development of new policies with existing guidelines and policies for the organization or constituency. For example, if the physical security policy requires that a certain set of predetermined individuals such as law enforcement, corporate security managers, public relations, or high-level management staff must be contacted during a breach; then look to build your CSIRT notification policies to match such guidelines.

As your CSIRT starts operation, think about having your staff document the steps they take to perform different actions. This can help keep a record of your processes and expand the initial set of policies and procedures created.

Sample Policies

Your CSIRT policies may include

- security policy
- open reporting environment policy
- incident reporting policy
- incident handling policy
- external communications policy
- media relations policy
- information disclosure policy
- information distribution policy
- human error policy
- training and education policy



Policies must be clearly understood so that staff can correctly implement procedures and enact their responsibilities.

All policies must

- have management approval and oversight
- be flexible for the CSIRT environment
- be clear, concise, and implementable
- be easy for new staff members to understand

Policies can be global or service-specific.

Other policies may need to be developed to determine when, how, and to whom, reports are escalated. Policies will also need to be developed for how and when your CSIRT will contact and work with law enforcement.

Example: CSIRT Acceptable Use Policy

Ensure it covers

- the appropriate use of systems
 - can systems be used for personal activities
 - what sites can and can not be connected to from CSIRT systems
 - if personal software can be downloaded and installed
- required security configurations for software, including browsers
- how backups are done and who has the responsibility for performing them.
- what type of virus scanning software should be used and corresponding configurations and procedures should be followed
- how software updates and patches are implemented
- what type of remote access is required for CSIRT services



One of the policies that a CSIRT should consider establishing is an Acceptable Use Policy that outlines how staff can use work and home equipment provided by the CSIRT or connected to the CSIRT network.

Are CSIRT staff the administrators of their own systems? Or is there someone else on staff that handles keeping systems up to date with software and patches?

Example: CSIRT Information Disclosure Policy

Ensure it covers

- categories of information
- what information can be released publicly
- what information can not be released
- who is authorized to receive each category of information
- what to do with questions from the media



Sample Procedures

CSIRT procedures can include but are not limited to

- standard operating procedures (SOPs)
- accepting and tracking incident reports
- incident and vulnerability handling
- answering the hotline
- gathering, securing, and preserving evidence
- configuring CSIRT networks and systems
- performing system and network monitoring and intrusion detection
- backing up and storing incident data
- notifying others (how information is packaged, distributed, archived, etc.)
- training and mentoring



If policies describe what you want to do, procedures provide the step-by-step instructions for how the policy or action will be implemented. Procedures complement policies by describing how the policy will work on a day-to-day basis.

Procedures will be very specific to the staff, environment, organization, and mission and goals of a CSIRT. Many of these procedures cannot be developed until the team is implemented.

Along with creating organizational procedures management must also decide who will create the procedures and where they will reside.

Procedures need to

- clearly specify how policies, services, and responsibilities are to be carried out
- provide the necessary level of detail to ensure clarity and prevent ambiguity
- have an associated glossary of local terms and definitions to enable new staff to understand them easily
- have an assigned maintainer and undergo a regular review and update cycle
- undergo testing for validity and usability

It is extremely important to test your procedures to see if they work in your CSIRT environment.

Test Your Policies and Procedures

Review policies and procedures after an actual incident.

- Did the needed policies and procedures exist?
- Were they easy to find?
- Were they easy to follow?
- Were they actually followed?
- Did they make sense for what actually happened?

If any of the above receive a “No” response, the policies and procedures should be reviewed for appropriate clarification, updates, amendments, or deletions.



There may be changes in your CSIRT structure and organization that will affect what is written in your policies and procedures. You may want to review your policies and procedures on an annual basis to ensure they are consistent.

One method of testing procedures is to have new staff review them and compare them to the processes they are being taught in their initial training. If procedures need to be changed, new staff can be used to update the procedure.

Some example resources are listed below:

EDUCAUSE/Cornell Institute for Computer Policy and Law

<http://www.educause.edu/icpl/>

SANS Security Policy Project

<http://www.sans.org/resources/policies/>

Site Security Handbook (RFC2196)

<http://www.ietf.org/rfc/rfc2196.txt>

Hire the Right Staff

Incident response staff must have the right combination of skills to be able to work with other team members and within your constituency.

These include:

- personal communication skills
- technical skills
- security and incident response skills



Hiring or obtaining the right staff is critical to the success of your CSIRT team.

Our experience and the experience of other CSIRTs has shown that the best staff have a variety of skills. They are dedicated, innovative, detail-oriented, flexible, analytical, problem-solvers, good communicators, and able to handle stressful situations. In talking with other CSIRTs one of the most important traits a team member must have is integrity. They must also have a good sense of being part of a working team. Staff must be able to deal with the slow days and the hectic days.

Skills will include:

- Personal
 - people skills
 - communication skills
- Technical
 - system and network administration experience
 - platform expertise: UNIX, Windows, Macintosh
 - basic understanding of Internet protocols
 - basic understanding of common computer attacks and vulnerabilities
- Security Training
 - incident handling experience
 - problem solving abilities

CSIRT Staffing Issues

Defining job functions and roles

Special hiring requirements

- Certifications or professional licenses
- Security clearances
- Service level agreements (SLAs)
- Data protection agreements
- Non-disclosure agreements

Recruiting and interviewing candidates

Mentoring and training

On-going professional development

Terminating CSIRT personnel



Software Engineering Institute | Carnegie Mellon

83

Will you require any certifications or special training for CSIRT staff? (such as the CERT® Certified Computer Security Incident Handler, CISSP, SANS or other certifications that may be required by an agency or military component)

Do you have any requirements that staff must first obtain a security clearance?

Be aware of the need for service level agreements and data protection agreements with contractors and managed service providers.

Suggested reading:

- Outsourcing Managed Security Services
<http://www.sei.cmu.edu/publications/documents/sims/sim012.html>

Options for Finding Staff

Finding staff for your CSIRT can be one of your toughest management tasks.

Do you hire new staff or train existing staff?

CSIRTs must be inventive in making jobs attractive

Promote job opportunities as benefits

- tuition reimbursement
- international travel
- conferences and seminars
- access to the latest tools and information
- job flexibility



Software Engineering Institute | Carnegie Mellon

84

When creating a CSIRT, one of the most important questions you must answer will concern where and how you will obtain your staff. Each of the below options can have benefits and drawbacks.

- Hiring dedicated CSIRT staff
 - Some CSIRTs look for staff with system and network administration skills and train them on the security aspects of working with a CSIRT. Others look for experienced incident handling staff.
- Using existing staff
 - They will be familiar with the existing systems and understand organizational policies, procedures, and business functions. Existing staff may not be able to perform their regular work and effectively perform incident handling tasks. They may also not have the necessary skills that you need.
- Outsourcing
 - Many organizations offer incident response services today that can help provide expertise that is lacking in your organization. Rates can be expensive. You must also worry about the security of your incident data. Outsourcing to multiple companies may make it difficult to share data.
- Hiring contractors
 - This is another way to supplement your staff and expertise. Again, you may not be able to find enough affordable contractors. Rates can also be expensive and you need to ensure that you have contractors that are loyal and dedicated to your mission.

Types of CSIRT Roles

Core Staff

- manager or team lead
- assistant managers, supervisors, or group leaders
- hotline, help desk, or triage staff
- incident handlers
- vulnerability handlers
- artifact analysis staff
- forensic analysts
- platform specialists
- trainers
- technology watch

Extended Staff

- support staff
- technical writers
- network or system administrators for CSIRT infrastructure
- programmers or developers (to build CSIRT tools)
- web developers and maintainers
- media relations
- legal or paralegal staff or liaison
- law enforcement staff or liaison
- auditors or quality assurance staff
- marketing staff



A CSIRT may find that it has the need for its own public relations, technical writing, or infrastructure staff. It may also be able to use resources from the parent organization or constituency.

You may also have staff that can perform multiple functions.

If your budget allows, you may be able to hire staff to match the skill sets needed for the services you provide. If you cannot find staff with those skills, you may need to train them yourselves.

Consider the type of training that new staff will need about your

- constituency and constituency's systems and operations
- standard operating procedures and policies
- information disclosure policy
- equipment and network acceptable use policy

You can take advantage of third-party courses to help train your staff:

- NSS and CERT/CC Managers, Technical Staff, and Incident Handler Courses
- SANS GIAC Certification and Training Program

Recognize that there are not enough experienced incident handlers to fill many of the currently available computer security positions; you are competing with other organizations for these valuable and limited resources. Some universities are now offering programs in information assurance and cyber security to expand the pool of educated people in these areas..

Build a Staff Training and Mentoring Plan

Determine staffing requirements based on the type and level of services being offered.

One best practice is to identify the types of roles or positions your CSIRT will need.

Once this is done, identify the knowledge, skills, and abilities that will be required for that position.

When those have been defined, then identify a training and mentoring strategy to ensure that each staff member hired receives consistent information and experience.



Once hired, the candidate should undergo a formal training schedule to become a productive member of the team. This should include a 2-6 month mentoring program, depending on the amount of expertise they already have. The mentoring program should cover

- first day knowledge
- the team's activities, roles, and responsibilities
- the mission and goals of the parent organization
- organizational policies and procedures

Any training and mentoring should help the new hire

- understand the team's mission and goals
- understand the policies and procedures to be followed
- know what tools and applications are available
- understand the critical services and data of the constituency that needs to be protected

Example: Specific CSIRT Positions

Incident Analyst Requirements

- Receive and Analyze network alerts from various sources and determine possible causes of such alerts
- Coordinate with IA staff to validate network alerts
- Perform analysis of log files from a variety of sources, to include individual host logs, network traffic logs, firewall logs, and intrusion detection system logs
- Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
- Monitor external data sources (e.g., vendor sites, CERT/CC, SANS, Security Focus, other public sources, etc.) to maintain currency of IA threat condition and determine which security issues may have an impact on the constituency
- Construct signatures which can be implemented on network tools in response to new or observed threats
- Perform event correlation, using information gathered from a variety of sources, to gain situational awareness and determine the effectiveness of an observed attack
- Notify managers, incident responders, and other team members of suspected/validated IA incidents and articulate the event's history, status, and potential impact for further action

Incident Responder Requirements

- Perform incident triage to include determining scope, urgency, and potential impact and identify and recommend specific remediation strategies
- Coordinate with and provide expert technical support to resolve incidents
- Track and document incidents from initial detection through final resolution
- Correlate incident data and perform trend analysis and reporting
- Serve as technical experts/liaisons to law enforcement personnel; explain incident details, provide testimony, etc.
- Write and publish guidance and reports on incident findings to constituency
- Perform initial collection of forensic images and inspect to discern possible mitigation or remediation on enclave systems
- Perform real-time Incident Handling (forensic collections, intrusion correlation/tracking, system remediation, etc.) tasks
- Collect and analyze intrusion artifacts (malware, Trojans, etc.) and use discovered data to mitigate potential IA incidents



Implement a Secure Infrastructure

A CSIRT infrastructure should incorporate all known precautions that are physically and financially possible.

- CSIRTs serve as a model to other organizations.
- To that end it is important that they ensure that their operations are secure and all incident and sensitive data is protected.

This should include both physical and network infrastructures.



Secure CSIRT Facilities

The physical location of your CSIRT is also important:

- not only for having a working space
- but also for protecting access to the CSIRT area

CSIRT location or working space might include:

- a general office area
- secure physical area for meetings and incident work
- a lab or test network area
- evidence room
- secure server room

Mechanisms should be in place to limit access to CSIRT staff

- badges or key card access
- access restrictions on staff who may enter area
- separate area with locked door for staff



CSIRT facilities and network and telecommunications infrastructure must be designed with great care to not only protect the sensitive data collected by the CSIRT but also to protect the CSIRT staff.

Thought should be given to locating CSIRT staff in offices with doors rather than cubicles. This will reduce the chance of sensitive information been overheard or seen.

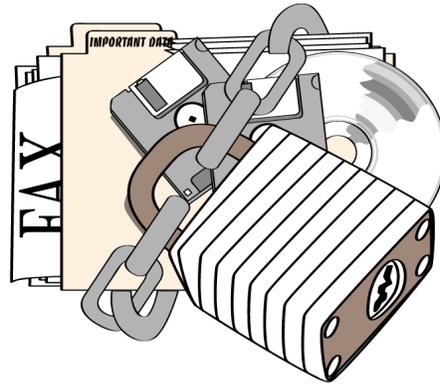
Many organizations today are placing staff in open cubicles in open areas of the office. Such placement can jeopardize the work that the team does by allowing for easy access to staff and therefore easy interruptions. It also places heavy requirements on staff to constantly protect the data they are working with. In such a configuration

- staff will need to lock file cabinets and desktop devices whenever they are away from their cubicle
- staff will need to remove all sensitive information from their desktop whenever they are away from their desk (clean desk policy)
- Staff will need to be very cognizant about who is around when they are talking about incident work
- monitors should be located so they do not face into open areas

Determine Security Needs

The following types of data should be secured:

- incident reports
- email
- vulnerability reports
- notes
- faxes
- encryption keys
- CSIRT publications



Most of your CSIRT data probably should be handled much more securely than other data, simply because of its sensitivity.

A CSIRT must secure incident information and other sensitive data because of

- legal requirements
- constituency expectations
- business necessity
- potential intruder threat

Other data to secure can include your publicly available information—to ensure that no unauthorized access and/or changes can occur (e.g., on a Web site.)

Sensitive data should

- be created/received in a secure area
- remain in a secure area

Data generated outside or leaving the secure area should be

- encrypted
- shredded
- in the custody of an employee

Select a location to store sensitive data such as a secure room, safe, or locked filing cabinet. Determine who should have access to the data.

Ensure access is restricted to authorized personnel only.

Define a Secure Area

Sensitive data should

- be created/received in a secure area
- remain in a secure area

Data generated outside or leaving the secure area should be

- encrypted
- shredded
- in the custody of an authorized employee
- handled securely

Identify a location to store sensitive data.

- secure room
- safe
- locked filing cabinet

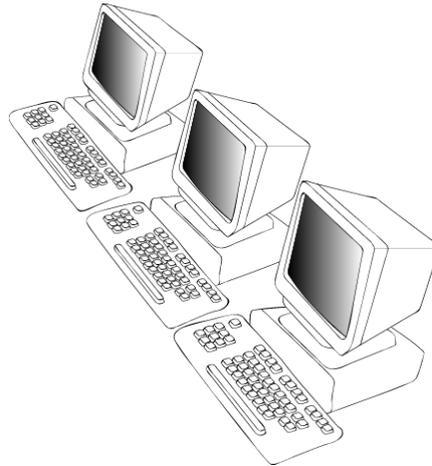
Determine who should have access to the data.



Determine CSIRT Equipment

CSIRT staff will need access to basic computing and communications systems to perform their functions.

- think about equipment for home and office
- home equipment will also need to be secured



CSIRT staff will need equipment for the various functions they perform. This might include the following:

- access to secure telephones, faxes, and any CSIRT or constituency intranet or extranet
- work equipment
 - telephones
 - office computing systems
 - laptops, projectors
 - notification systems - cellular telephones, pagers, etc.
 - shredding machines
 - electronic whiteboards

You may also need to provide home equipment for CSIRT staff depending on the types of services you are providing and the availability of those services.

Home equipment will also require a secure infrastructure - including appropriate firewalls and secure communications systems—such as VPNs, ssh, or digital certificates.

Staff may also need to have additional telephone lines, mobile devices (phones, blackberries, two-way radios, etc.).

Determine CSIRT Network Services and Systems

Recommendations and considerations include

- separate CSIRT network
- secure network and system configurations
- separate email, web, DNS, and other appropriate servers and services
- up-to-date and consistent software versions and patches
- method for updating software on staff devices in a standardized fashion
- test network, lab, or devices
- secure intranet for CSIRT staff
- robust tracking system for incident handling
- secure communications mechanism
- secure remote access
- phone bridges and teleconferencing capabilities
- analog and digital phone access



It is a recommended practice to separate or isolate the CSIRT infrastructure from other parts of the organization to protect data and to protect access to CSIRT staff. This may include

- using a firewall between the CSIRT and other units
- creating separate services (email, FTP, webserver, DNS, backup, etc.)
- limiting physical access to CSIRT staff areas and systems
- creating a separate "DMZ" area for public access

Ensure hosts and network devices are up to date with the latest security patches

- configure hosts and network devices (routers, switches, hubs, firewalls, etc.) securely
- limit access through access control lists (ACLs) on hosts and network devices
- configure monitoring, auditing, and logging facilities
- secure all media (floppy disks, tapes, etc.)

All staff should understand what software is appropriate to use on CSIRT systems. Applications and software with known security holes and flaws should not be permitted. Guidelines on how CSIRT systems should be used may also be necessary; including guidance on opening attachments and visiting certain sites.

Never perform any vulnerability testing, artifact analysis or other testing on production systems. All such analysis should be done in a test lab or network.

Where possible the test network or lab should contain

- hardware platforms to match what is used by the constituency
- operating systems and software to match what is used by the constituency
- network devices to match what is used by the constituency

Install Network and System Defenses

As a CSIRT, you may be a target for attack.

Monitor your network and systems using

- virus protection and scanning software
- network security scanners
- intrusion detection and prevention systems (IDS/IPS)



A set of CERT security practices has been compiled in The CERT® Guide to System and Network Security Practices, published by Addison-Wesley. It is available for purchase at walk-in and online bookstores.

Firewalls should have the following enabled

- egress/ingress filtering where/when appropriate
- logging and alert mechanisms

Be Prepared for Emergency Situations

Ensure data is protected in case of

- fire
- flood
- tornado
- intruder compromises

Trusted copies of original media for all software should be kept in a secure location.

Backups should be stored in multiple locations.

HVAC (heating, ventilation, and air conditioning) issues should be taken into consideration.

Install protected power supplies and backup generators.



Do doors to secure areas automatically unlock in case of a fire or power failure? If so, what is the security implication for protection of information in that area?

Where appropriate consider encrypting backups, especially if archived by external third-party providers. Periodically check viability of backups to ensure they continue to be readable.

Develop a CSIRT Disaster Recovery Plan

If your CSIRT facilities were suddenly inoperable or inaccessible, could your CSIRT still function?

- Do you have a disaster recovery or business resumption plan?
 - Have you tested it?
- Do you have a secured backup location?
 - Have you tested it?
- Do you have mirrored sites for important resources and services?

Have you identified the critical services that must be operational in an emergency?



You may be able to negotiate arrangements with another, trusted CSIRT to mirror important public services you provide.



Incident Management Processes:

- *Introduction*
- Prepare/Sustain/Improve*
- Protect Infrastructure*
- Detect Events*
- Triage Events*
- Respond*

CERT |  Software Engineering Institute | Carnegie Mellon 97

Building Your Incident Management Plan

Your IM plan details what IM processes are performed across your enterprise including

- *relationships between processes*
- *who performs them*
- *existing interfaces*
- *inputs and outputs*

What should be in your IM plan?

- organizational group responsible for each IM function
- detailed roles and responsibilities
- defined interfaces between functions
- defined event and incident criteria
- point of contact for reporting events and incidents
- timeframe for reporting and handling incidents
- workflows for handling incidents
- emergency situations
- response actions for specific types of incidents
- postmortems and feedback activities



What should be in your IM plan?

- an explanation of the existing IM capability and services
- a list of the functions of the incident management process and what part of the organization is responsible for each
- a more detailed breakdown of roles and responsibilities for who performs what functions in what timeframes and any exceptions
- a defined criteria for what constitutes an event and incident
- timeframes for reporting and handling incidents
- the workflow, process flow, or even flow chart of how an incident passes through the processes

To define the various enterprise wide incident management functions you can use

- The Incident Management Process Model process and subprocesses and workflows
- The Incident Management Capability Metrics service categories and metrics indicators
- The Resiliency Engineering Framework capabilities and sub-practices
- other benchmarks or standards

What Supports Your IM Plan?

Governance support of IM plan

Recognition of the importance of IM

Risk analysis and resulting output

Information classification scheme

Incident criteria

- Definition of incident
- Prioritization
- Categorization
- Escalation

Incident reporting policy, guidelines and reporting template

Critical systems and data inventories

Guidelines for handling Personally Identifiable Information (PII)



Much of what supports your incident management plan must be determined by the organization itself. The IM components or CSIRT must work with others in the organization to identify and institutionalize these supporting activities.

Various types of risk analysis methodologies or industry standards for computer security practices exist. Organizations should evaluate which ones will work best for their structure. Examples include the following:

- CCTA Risk Analysis and Management Method (CRAMM)
- Commonly Accepted Security Practices and Regulations (CASPR)
- Control Objectives for Information and (Related) Technology (COBIT)
- Methode d' Evaluation de la Vulnerabilite Residuelle des Systemes d'Informa (MELISA)
- Information Security Forum's Fundamental Information Risk Management (FIRM)
- ISO 13335, Information Technology – Guidelines for the Management of IT Security
- ISO 27001, Information technology - Security techniques - Code of practice for information security management
- ISO 21827, Maturity Model (SSE-CMM®)
- ISO 15408, Information Technology – Security Techniques – Evaluation Criteria for IT Security.
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), information is available at

<http://www.cert.org/octave/>

Information to help benchmark your critical assets can be found in the publication, The Critical Success Factor Method, Establishing a Foundation for Enterprise Security Management. This is available at

<http://www.cert.org/archive/pdf/04tr010.pdf>

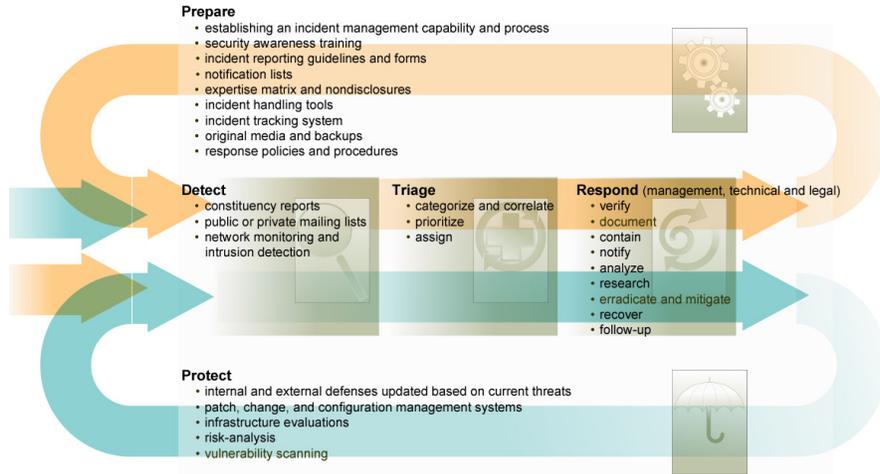


Incident Management Processes:

- Introduction*
-  *Prepare/Sustain/Improve*
- Protect Infrastructure*
- Detect Events*
- Triage Events*
- Respond*

CERT |  Software Engineering Institute | Carnegie Mellon 100

Incident Response Starts Before an Incident Occurs



Effective response starts long before you actually have an incident to handle. Proactively you can aid the response process by having people, processes, technology, facilities, and information in place. You also need to prepare your staff and constituency through the provision of computer security training and reporting guidelines. You need to have good computer security incident detection processes and tools in place. You should also include a process for improving your security posture and policies based on what you learn during an event or security incident.

You need to have your incident management plan in place.

Mission of the Prepare Process

To *create* an incident management capability that supports the mission and goals of the constituency.

To *improve and/or sustain* an existing incident management capability that supports the mission and goals of the constituency.



The Prepare/Sustain/Improve Process

The Prepare/Sustain/Improve process contains a number of subprocesses to

- Coordinate Planning and Design
 - Identify CSIRT requirements
 - Establish CSIRT vision
 - Obtain Sponsorship and Funding for the CSIRT
 - Develop CSIRT Implementation Plan
- Coordinate Implementation
 - Develop CSIRT Policies, Procedures, and Plans
 - Establish CSIRT Incident Management Criteria
 - Deploy Defined CSIRT Resources
- Evaluate CSIRT Capability
 - Conduct Postmortem Review
 - Determine CSIRT Process Modifications
 - Implement CSIRT Process Modifications



We discussed most of the Prepare/Sustain/improve process in the earlier part of this morning's class.

Improvement comes from two subprocesses

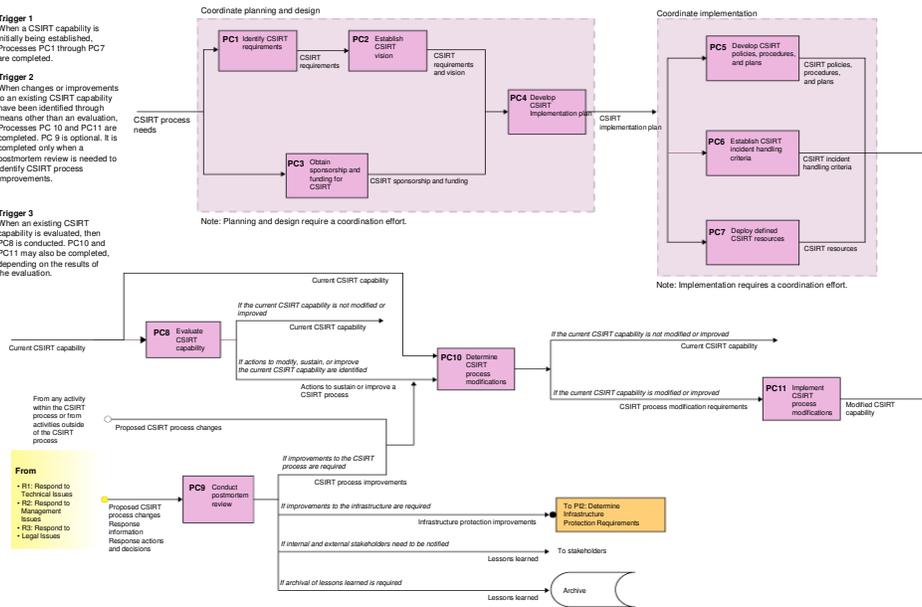
- Evaluate CSIRT Capability
- Conduct Postmortem Review

PC: Prepare, Sustain, and Improve CSIRT Process

Trigger 1
When a CSIRT capability is initially being established, Processes PC1 through PC7 are completed.

Trigger 2
When changes or improvements to an existing CSIRT capability have been identified through means other than an evaluation, Processes PC 10 and PC11 are completed. PC 9 is optional. It is completed only when a postmortem review is needed to identify CSIRT process improvements.

Trigger 3
When an existing CSIRT capability is evaluated, then PC8 is conducted. PC10 and PC11 may also be completed, depending on the results of the evaluation.



The Prepare/Sustain/Improve process contains a set of subprocesses that describes the planning and design phase (PC1-PC3) of the CSIRT or incident management process, along with defining the initial implementation plan (PC4). These are used to build, staff and equipment the capability (PC5-PC7) and later to evaluate or conduct post mortems (PC9)—which then cycle back into sustaining and improving the capability.

Other subprocesses focus on the sustainment and improvement of an existing capability (PC8, PC10, PC11).

Who is Involved in the Prepare/Sustain/Improve Process?

This process may include a variety of different staff with different roles and responsibilities:

- Development team (key stakeholders)
- Senior managers, business owners/operators
- IT system and network operations staff
- Administrative operational staff
- Constituency representatives
- CSIRT staff
- Other relevant parties, as appropriate
 - Legal
 - Human resources
 - Public relations
 - Law enforcement
 - External third-party providers (MSSPs)
 - Subject matter experts



Designated staff are involved in

- Identifying the CSIRT requirements
- Establishing and refining the CSIRT vision
- Obtaining sponsorship and funding for the CSIRT
- Developing the CSIRT implementation plan

Best Practices

Performing incident management as efficiently and effectively as possible may require various decisions to be made ahead of time.

This can include determining if and when

- law enforcement will be involved
- forensics evidence will be collected
- systems can be isolated or shutdown

It can also include identifying

- a communications plan
- points of contact with other internal and external groups
- secure communication mechanisms
- data classifications of materials handled

And having access to

- critical system inventory information
- network topologies
- network baselines



It will help if predetermined criteria or decisions have been made on the types of reports and requests that will require

- evidence to be collected (computer forensics)
- law enforcement to be called
- reporting to be made to another entity



Incident Management Processes:

- Introduction*
- Prepare/Sustain/Improve*
-  *Protect Infrastructure*
- Detect Events*
- Triage Events*
- Respond*

CERT |  Software Engineering Institute | Carnegie Mellon 107

Mission of the Protect Process

To adequately protect and secure critical data and the computing infrastructure of the CSIRT and its constituency

- in response to current risk, threats, attacks
- in response to proposed improvements
- based on a predetermined schedule
- while handling information within the appropriate security context



Protect Infrastructure (Protect), which includes subprocesses to

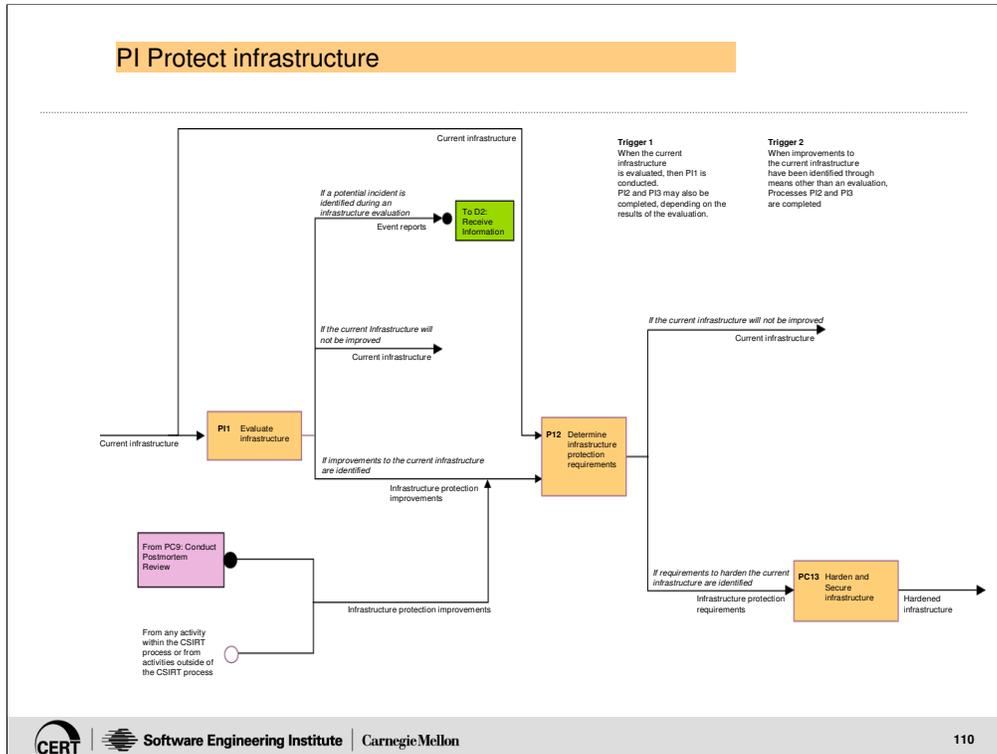
- implement changes to the computing infrastructure to stop or mitigate an ongoing incident or to stop or mitigate the potential exploitation of a vulnerability in the hardware or software infrastructure
- implement infrastructure protection improvements resulting from postmortem reviews or other process improvement mechanisms
- evaluate the computing infrastructure by performing such tasks as proactive scanning and network monitoring, and by performing security and risk evaluations
- pass off to the Detect process any information about ongoing incidents, discovered vulnerabilities, or other security-related events that were uncovered during the evaluation

The Protect Process

The Protect process involves subprocesses to

- respond to ongoing threats
- prevent incidents from occurring or repeating





The Protect process, outlined in this workflow diagram, contains a set of subprocesses that describes the activities involved in proactive protection of infrastructures. These include subprocesses to evaluate the current infrastructure (P11) or receive infrastructure protection improvements from any process within the incident management functions or outside those functions. Once the infrastructure protection improvements are reviewed, the modifications that need to be made are determined (P12) and implemented as appropriate (P13).

Protecting Against Incidents

Protection includes incorporating strategies to protect or defend the organization's systems and networks against misuse, attacks, threats, and failures.

This can include following standards and best practices for protecting systems and networks, such as:

- implementing defense-in-depth protection strategies
- implementing robust and automated patch management and anti-virus mechanisms
- evaluating the security of the infrastructure
 - network monitoring
 - vulnerability scanning
 - penetration testing
 - risk analysis
- providing security awareness and training
- reviewing and validating policies, procedures, guidelines



The implementation of best practices for the protection of systems and networks (based on the relevant standard of due care, whether ISO 27002 or other standards or regulatory requirements) ultimately improves protection of systems and reduces the number of incidents that must be handled.

The following list is a sample of some of the available standards and best practices that exist:

- ISO 27002 - Information technology - Security techniques - Code of practice for information security management
- Control Objectives for Information and related Technology (COBIT)
- Federal Financial Institutions Examination Council (FFIEC) Handbooks
- (ISC)2 CISSP Body of Knowledge (International Information Systems Security Certification Consortium; Certified Information Systems Security Professional)
- Information Security Forum Best Practices
- Information Systems Security Association; Generally Accepted Information Security Principles (ISSA GAISP)
- Information Technology Governance Institute (ITGI) sources
- Information Technology Infrastructure Library (ITIL)
- National Institute of Standards and Technology (NIST) (selected SP 800 series); FIPS 199
- National Cyber Security Summit Task Force reports
- SEI body of work including Capability Maturity Model (CMM), Capability Maturity Model Integration (CMMI), OCTAVE, Security Knowledge in Practice (SKiP), CERT Security Practices

Who Performs the Protect Process

Based on organizational mission and assigned job responsibilities for security and incident management, the protect subprocesses could be performed by a variety of personnel.

This could include

- IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators)
- CSIRT staff
- third-party contractors or service providers (MSSPs or ISPs)
- auditors, risk management staff, compliance staff or independent evaluators



The actual hardening and securing of the infrastructure could be performed by IT staff, designated CSIRT staff, third-party contractors or service providers. These same personnel may be involved in developing the requirements for improving the infrastructure.

Evaluation of the infrastructure could be performed by those same personnel, along with auditors, risk management staff, compliance staff, and third party or independent evaluators.

Best Practices

IM or CSIRT staff should share data and guidance with IT and infrastructure staff.

IM capability or CSIRT representation should be implemented on any

- organizational security councils or boards
- change management boards or committees
- technology review committees
- other security groups or boards

IM and CSIRT staff should have a means to provide input into

- configuration management decisions
- patch management actions
- new software and hardware installation
- network defense strategies and configurations





Incident Management Processes:

- Introduction*
- Prepare/Sustain/Improve*
- Protect Infrastructure*
-  *Detect Events*
- Triage Events*
- Respond*

  Software Engineering Institute | Carnegie Mellon 114

Mission of the Detect Process

To identify unusual activity that might compromise the mission of the CSIRT constituency and/or the CSIRT

- within defined time constraints
- while handling information within the appropriate security context

The activity or information, once detected, is passed on to the Triage process as a report, alert, or similar notification.



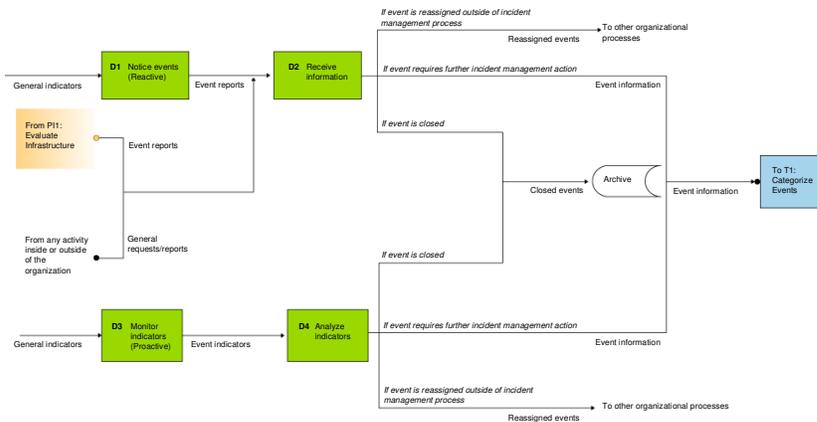
The Detect Process

In the Detect process, information about potential incidents, vulnerabilities, or other computer security or incident management information is gathered in two ways

- reactively
- proactively



D: Detect Events



In the Detect process, information can be obtained “reactively” from a variety of sources: constituent reports, reports or notifications from other external parties (another CSIRT, for example) (D1, D2) or proactively (D3), such as alerts from intrusion detection systems, intrusion protection systems, other monitoring devices (logs from firewalls, netflows, etc.). Information is analyzed (D4) and passed on for appropriate handling (or closed if no further action is warranted).

Reactive Detection

In reactive detection, information can be detected and reported from two main sources:

- system users
- other computer security experts such as an external CSIRT, coordinating CSIRT, or a security organization

Information may enter the detect process via

- phone call or FAX
- email or mailing list
- web-form
- walk-in
- intrusion detection alert



In reactive detection, information is received from internal or external sources in the form of reports or notifications.

- Those using the computer facilities of the organization may notice some unusual or malicious activity and report this to the appropriate contact point. The reporting may involve submitting an incident reporting form or calling the appropriate point of contact, such as a help desk or a CSIRT hotline.
- Other computer security experts, may send an alert or notification that must be assessed to see if there is a potential threat to the receiver's infrastructure. For example, AusCERT might receive reports of a new worm propagating in the Asia Pacific area. They would create an advisory or alert and send it out to a subscriber mailing list. Another CSIRT on this list, or even a security management team on this list, would receive the alert via email.

Proactive Detection

Proactive detection involves monitoring indicators of possible incidents or the exploitation of vulnerabilities through mechanisms such as:

- network monitoring
- vulnerability scanning
- host scanning
- virus checking
- technology watch
- situational awareness
- risk analysis or security audit



Proactive detection requires actions by the designated staff to identify suspicious activity. Staff proactively monitor a variety of data (such as host logs, firewall logs, and netflows) and use intrusion detection software to monitor network behavior, looking for indications of suspicious activity (D3). The data are analyzed and any unusual or suspicious event information is forwarded to the Triage process.

For example, staff performing such activity may be within or outside of a CSIRT function. Often it is the IT or network operations staff that performs this function and passes on any suspicious activity or relevant incident or vulnerability information to the Triage process. In such cases it is important to already have procedures established for passing on this information. Staff doing this monitoring need some criteria to follow to help them determine what type of alerts or suspicious activity should be passed on as a report to Triage. [If a possible event is indicated, the event information is sent to the Triage process. If the information does not indicate an event that needs action, the event is closed.

Proactive detection also includes technology watch or public monitoring functions. These activities are defined as services in CSIRT Services, available at

<http://www.cert.org/csirts/>

These services involve looking at available security resources such as mailing lists, web sites, articles, or news reports that are available publicly for free or from a commercial service for a fee. Staff performing technology watch functions can include actual CSIRT staff, network operations staff, other systems and network administrators, or even outsourced contractors. Information sought and passed to Triage could include new vulnerabilities, new attack types and threats, new recommendations and solutions for preventing incidents, or general political, social, or sector-related information that may have relevance to any ongoing or potential malicious activity.

Who Performs the Detect Process?

Based on organizational mission and assigned job responsibilities for incident management, the detect subprocesses could be performed by a variety of personnel, such as:

- designated CSIRT staff
- members of the CSIRT constituency
- victim or involved sites
- IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators)
- trusted external groups (other CSIRTs, vendors, etc.)
- external groups (third-party reporters, MSSPs, media, law enforcement)



Other personnel reporting reactively may include

- help desk staff
- CSIRT triage staff
- CSIRT hotline staff
- CSIRT manager
- incident handlers
- information security officer
- system and network administrators
- third-party answering service
- coordination center

Personnel for proactive monitoring can include

- IT staff (e.g., NIC/NOC/SOC staff, system and network administrators)
- selected members of the CSIRT staff
- third parties (e.g., MSSPs, collaborators, ISPs, trusted subject matter experts)
- coordination center

Best Practices

Implement mechanisms to support incident detection, reporting, and tracking.

These can include

- incident reporting guidelines
- incident reporting forms
- incident reporting tracking system
- team email address
- hotline or helpdesk
- public monitoring
- knowledge management system
- network monitoring



Incident Reporting Guidelines

Incident reporting guidelines can include

- the definition of an incident for your constituency
- an explanation for why an individual or group should report incident activity
- the identification to whom or where the report should be sent
- an explanation of how to report
- a description of what should be included in a report
- an explanation of when to report



Your incident reporting guidelines can be used to define what an incident is for your organization or constituency. This may include

- categories of incidents
- priorities associated with incident types

You can also use them to explain why people should report to your CSIRT.

- There are several reasons to report an incident to a CSIRT. The team may be able to provide technical assistance in responding to the incident, or put you in touch with other sites involved in the same activity. The reports allow the CSIRT to collect and distribute better information about intruder activity throughout the constituency. Reporting incidents to a CSIRT helps to promote greater security awareness and improve the security of the Internet. Your organizational policies or local laws may require you to report the activity.

The guidelines can be used to explain

- who should receive the reports: the CSIRT directly, a centralized helpdesk, or some other group
- the exact method and procedures for submitting the information: via a form, via email, via phone calls
 - contact information
 - time and date of report
 - timeframe and date of activity
 - systems affected [OS version, patch level, purpose]
 - brief description of problem or activity
- any time requirements for submitting reports

The CERT/CC provides a set of incident reporting guidelines that can be followed to understand what, when, and how, incident activity should be reported. These guidelines are available at:

http://www.cert.org/tech_tips/incident_reporting.html

Incident Reporting Forms

Reporting forms can be used for incidents, vulnerabilities, and other request types.

Use of a reporting form helps sites to

- provide the appropriate information
- organize the information they provide
- understand how to make a request/report

Use of a reporting form helps CSIRTs to

- prioritize reports
- obtain the information needed in one interaction
- set expectations of sites using the form



Sample forms include

- CERT/CC Incident Reporting Form (IRF)
http://www.cert.org/reporting/incident_form.txt
- CERT/CC Vulnerability Reporting Form
http://www.cert.org/reporting/vulnerability_form.txt
- CERT/CC Incident Reporting Form (web-based)
<https://irf.cc.cert.org/>

Incident Reporting Tracking System

Decide what data your CSIRT needs to record and track to

- provide an effective response service
- fulfill management and funding needs
- generate trend and statistical information

Decide what type of system to use to record and store this data.

- database
- help ticket system
- text files
- log book

Ensure processes are available for capturing and storing data from

- telephone calls
- FAX messages
- other correspondence

Provide support for handling encrypted data.

- Decrypt internal copies of any encrypted information.
- Re-encrypt with an internal CSIRT key.



Ensure all data is recorded so that

- it can easily be searched
- anyone can pick up in the middle of an incident
- you can determine the current work load and its distribution

Incident Tracking System Sample Fields

Reference Numbers

Contact information

Date and time

- of report
- of activity
- of discovery

Description of problem

- category and priority
- overview
- in-depth technical information
- actions taken
- impact and scope

Systems affected

- owner
- criticality and mission
- software and patch versions

Assigned staff

Action items

Staff contacted or interviewed

Supplemental data gathered

Cost of damage

Cost of recovery

Time to resolve

Resolution



Team Email Address

Have a standard email address that is used to communicate with your team.

Ensure this is the address that is published for constituents to send reports or requests for information.



CSIRT Hotline or Helpdesk

General Hotline Issues

- Organizational location
- Staffing
- Hours of operation
- Level of service
- Required policies and procedures



Each CSIRT must decide how to provide their hotline service. Many teams do not have a formal CSIRT hotline but use an already existing organizational helpdesk number to receive computer security incident reports and requests.

Issues relating to where a hotline service is located in the CSIRT and parent organization, how the staffing is scheduled, what the hours of operation are and what level of services is provided at the hotline must be determined and documented in relevant policies and procedures.

Knowledge Management System

Such a system can be used to archive and organize public monitoring, vulnerability, and vendor security information in a way that is available to IM staff.

It can also be used to record standard responses given to various common questions.

It allows for searching and correlation of information.

It reduces duplicate storage and dissemination of information.



Public Monitoring

Public monitoring entails gathering information from public sources

- *incident activity*
- *vulnerability information*
- *artifacts*
- *situational awareness information*

There are five basic steps in public monitoring

- Identify information to collect.
- Gather information.
 - web sites
 - mailing lists
 - RSS channels
 - Others
- Evaluate information.
- Notify appropriate personnel
- Archive information in a knowledge management system.



Proactive detection also includes technology watch or public monitoring functions. These activities are defined as services in CSIRT Services (see Appendix B), available at

<http://www.cert.org/csirts/services.html>

These services involve looking at available security resources such as mailing lists, web sites, articles, or news reports that are available publicly for free or from a commercial service for a fee. Some sample resources include

- Security advisory web sites
 - **US-CERT, SecurityFocus, OSVDB, vendor web sites**
- Security related news web sites
 - **Slashdot, The Register,**
- Mailing lists
 - **Bugtraq, Full-Disclosure, Vuln-Dev, vendor announcements**
- Mailing list archives
 - **Neohapsis and MARC**

Public monitoring gathers information from public sources that is relevant to your constituency or CSIRT work. This information is used to

- keep up-to-date with ongoing security-related activities
- provide information on new vulnerabilities, attack types, mitigation strategies, and security tools
- provide insight, perspective, and context for ongoing activity

Situational Awareness

You need to know what is going on around you.

You need to correlate this information with any ongoing or suspicious system or network activity.

You need to use this information to make better decisions.

“**Situational awareness** is being aware of everything that is happening around oneself and the relative importance of everything observed — a constantly evolving picture of the state of the environment.”¹

In the computer security field, situational awareness relates to the collection and correlation of data and information from

- systems and networks
- incident and vulnerability reports
- news and current events



The term situational awareness actually came out of the aviation field. It is basically taking into account all the different environmental data around you and using it to make decisions. In the area of computer security, it focuses on examining sources of information that can have an effect on your CSIRT or constituency, and then using this information to predict future activity. Situational awareness provides a context for decision making.

Situational awareness includes collecting news information

- local, regional, national, and international news articles
- major economic, political, or social occurrences that might impact the evaluation of computer security events

¹ Source: http://en.wikipedia.org/wiki/Situational_awareness

Network Monitoring

Organizations must continually monitor their networks for suspicious or abnormal behavior.

- IDS/IPS
- netflows
- firewalls

Use centralized logging when possible.

Have a data retention policy.

Synchronize clocks.

Key data to log and track

- attempts to gain access through existing accounts
- failed file or resource access attempts
- unauthorized changes to users, groups and services
- systems most vulnerable to attack
- suspicious or unauthorized network traffic patterns

Source: SANS Top 5 Essential Log Reports



Suspicious or unauthorized network traffic patterns might include

- Inbound ICMP Host Unreachable Errors (Type 3s)
- Outbound ICMP time Exceeded in Transit Errors (Type 11s)
- Unexpected outbound DMZ traffic
- Outbound TCP/25 from a non-SMTP server
- Outbound Internet Relay Chat (6660-6669, 7000, Others)

Source: SANS Top 5 Essential Log Reports

http://www.sans.org/resources/top5_logreports.pdf



Incident Management Processes:

- Introduction*
- Prepare/Sustain/Improve*
- Protect Infrastructure*
- Detect Events*
-  *Triage Events*
- Respond*

CERT |  Software Engineering Institute | Carnegie Mellon 132

Mission of the Triage Process

To sort event information and assign it to appropriate personnel

- within defined time constraints
- while handling information within the appropriate security context
- while documenting information in an appropriate manner



Triage may be the first time information about an event or incident is documented and recorded. This documentation may also occur in the Detect process if information comes into a general helpdesk, for example.

The Triage Process

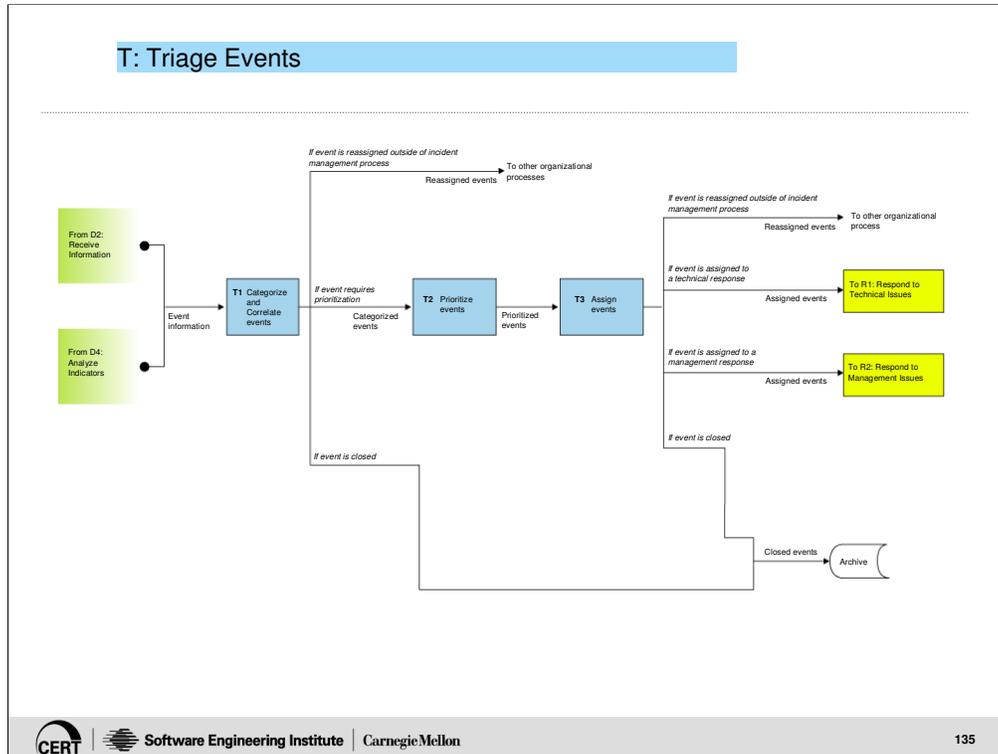
Triage is the

- single point of entry for all CSIRT correspondence and information
- mechanism and set of tools used to
 - categorize
 - correlate
 - prioritize
 - assign
- all incoming correspondence and reports



Triage is an essential element of any incident management capability, particularly for any established CSIRT. Triage is on the critical path for understanding what is being reported throughout the organization. It serves as the vehicle by which all information flows into a single point of contact, allowing for an enterprise view of ongoing activity and a comprehensive correlation of all reported data. Triage allows for an initial assessment of an incoming report and queues it for further handling. It also provides a venue for beginning the initial documentation and data entry of a report or request, if this has not already been done in the Detect process.

T: Triage Events



Triage is the process of sorting, categorizing, correlating (T1), prioritizing (T2), and assigning (T3) incoming events, incident reports, vulnerability reports, and other general information requests. It can be compared to triage in a hospital, where patients who need to be seen immediately are separated from those who can wait for assistance.

Who Performs Triage?

Based on organizational mission and assigned job responsibilities for incident management, the triage subprocesses could be performed by a variety of personnel.

This could include

- designated CSIRT triage staff
- CSIRT hotline staff
- other CSIRT staff such as incident handlers
- CSIRT Manager
- organizational helpdesk
- IT staff
- information security officer (ISO)
- external coordination center staff



Triage may be performed by a variety of personnel. Who performs it depends on the staff and job assignments within the incident management functions and across the organization. It also depends on the level of service provided by the Triage staff. For example, we have seen some organizations in which event reports come to an information security officer, who categorizes and prioritizes the event and contacts the appropriate personnel in the CSIRT to handle the event. In very small CSIRTs, it may be the CSIRT manager who receives the event report and who performs the triage functions. In a large multinational organization, it may be local IT help desks that receive the event information for triage. In a national CSIRT, it may be dedicated CSIRT staff that performs triage.

If Triage is performed outside of a CSIRT, particular attention must be paid to how the information is transferred to the CSIRT and what type of training is provided for those staff performing triage, so that they know what information should be passed to the CSIRT and in what format it should be passed. This is a key handoff interaction that, if done improperly, can cause a delayed response that can increase the amount of damage and impact resulting from an incident or delay further investigation of a report because it was not received in a timely manner.

What Questions are Addressed in Triage?

During the triage process, a number of questions are answered and first steps taken.

- What category and priority should a report or request be assigned?
- Is this a new report or is it related to ongoing activity?
- Are any preliminary actions required?
 - Decrypt information.
 - Virus check any attachments.
 - Distribute information to others on staff related to a hot site or ongoing communications.
- Who should handle this event or incident?



The Triage process involves a review of incoming information to determine its validity and to determine what type of event is being reported and what initial action to take.

It facilitates recognition and appropriate separation of

- new incidents
- new information for ongoing incidents
- information requests
- vulnerability reports
- other service requests

Triage provides access to the “bigger picture”.

Tactical Versus Strategic Triage

Triage can be performed at two different levels

- Tactical – focuses on the sorting and categorization and assignment of reports and requests based on pre-determined criteria
- Strategic – focuses on performing a true higher level assessment of the situation and determination of business impact

The level performed will impact the skill set required of the triage staff.

Strategic triage requires a good understanding of the critical business drivers for an organization or constituency.



Most important to how well Triage is executed is the expertise and skill level of the Triage staff. Triage is difficult to implement in an effective manner. Some organizations have devoted a lot of support and training to Triage, and they perform a higher level of analysis, a strategic assessment of the situation, rather than a tactical sorting of the information received. Depending on what role Triage plays in your incident management process—strategic or tactical—a different set of knowledge and skills is needed. Often Triage is assigned to a junior help desk person or a technician. Such a person may not have the required knowledge and skill to perform a true assessment of the situation. In that case the assessment is done in the Respond process, and Triage is used to simply sort, categorize, and assign the initial report.

If Triage is built to perform a true assessment function, staff must have the right mix of technical skills and business awareness skills. Business awareness means understanding the mission and purpose of the parent organization, understanding what systems and assets are critical to the achievement of this mission, and being able to determine what effect threats, malicious activity, and exploitation of vulnerabilities in the computing infrastructure will have on the overall operation of the business. This allows the true impact to the organization to be determined in the Triage process, which can decrease the time to respond to the event or incident.

Benefits of Triage

Triage provides

- an enterprise view of ongoing activity
- a central location for incident reports
- a comprehensive correlation of all reported data
- an initial assessment of an incoming report and queuing for further handling
- a mechanism to begin the documentation and data entry of a report or a request

Triage also facilitates

- work load balancing
- escalation of events or incidents
- training of new staff



The triage function provides an immediate snapshot of the current status of all activity reported—what reports are open or closed, what actions are pending, and how many of each type of report has been received. This process can help to identify potential security problems and prioritize the workload. Information gathered during triage can also be used to generate vulnerability and incident trends and statistics for upper management. Triage can be of particular importance when an emergency request occurs, as triage can involve processes to elevate the priority of a report, escalate the handling of the report, and notify relevant parties and stakeholders, especially in the case of a critical or major event.

If triage is not properly handled, it can be a single point of failure.

In times of crisis, triage may need to take place at a reduced level for low-priority services while remaining focused on high-priority service requests.

Triage can help provide training to new staff by serving as an entry level job. It gives staff an overview and understanding of CSIRT operations.

Activities Performed in Triage

Collecting critical information

Categorizing incoming event and incident reports (or other triaged information)

Correlating activity, to determine information about scope and severity, whether single or multiple occurrences of an event or incident

Prioritizing activity (based on predetermined set of criteria)

Assigning to appropriate personnel for further handling



The initial step, in the Triage process in our best practice incident management model, Categorize and Correlate Events (T1 in the workflow diagram), uses predefined criteria, if available, to classify the incoming events. (The predefined criteria is developed by the organization.)

For example CERT/CC uses established categories of Modus Operandi (MO)

- unknown
- user compromise
- root compromise
- misuse of resources
- denial of service
- reconnaissance

The Handbook of Legal Procedures – online database (2005) for the European Union developed by Rand uses the following categories of incidents

- Target fingerprinting
- Unauthorised access to transmission
- Unauthorised access to information
- Unauthorised modification of information
- Malicious code
- Denial of service
- Account compromise
- Intrusion attempt
- Unauthorised access to communications systems
- spam

Best Practices

The faster an analyst can assess the impact and effect of an incident, the faster it can be contained and handled.

The following make the Triage process more efficient

- critical asset inventory and evaluation
- shift logs and formalized handoffs
- ability to review incoming incidents in non-sequential order
- reference numbers
- special contact lists



The following make the Triage process more efficient

- critical asset inventory and evaluation – that allows you to identify the importance and priority of critical assets
- shift logs and formalized handoffs – if CSIRT or helpdesk has multiple shifts for a 24 hour operation this allows the current status major incidents or threats to be monitored
- ability to review incoming incidents in non-sequential order – this allows the highest priority or critical incidents to be handled first
- reference numbers – unique IDs for reported incidents
- special contact lists – list of constituents with special handling requirements

Special Contacts

Identify

- a list of “hot” customers, constituents, or collaborators who should receive immediate attention
- any other “regular” contacts who may (or may not) need immediate attention



Your special contacts list might include

- sponsors
- high-ranking officials
- other CSIRTs
- vendors who are currently working with you on a vulnerability analysis
- vendors whose products are affected by a new attack type
- other “regulars” (noted security experts, regular incident or vulnerability reporters, etc.)

Your special contacts list should be a dynamic document that can be easily updated. This is necessary, as the people on the list will change due to staff turnover, change in sponsorship, or priority of incident activity.



Incident Management Processes:

- Introduction*
- Prepare/Sustain/Improve*
- Protect Infrastructure*
- Detect Events*
- Triage Events*
-  *Respond*

CERT |  Software Engineering Institute | Carnegie Mellon 143

Mission of the Respond Process

To resolve events and incidents

- within defined time constraints
- while handling information appropriately (e.g., within security, legal, and investigative contexts)
- according to established policy, procedures, and quality requirements



The Respond Process

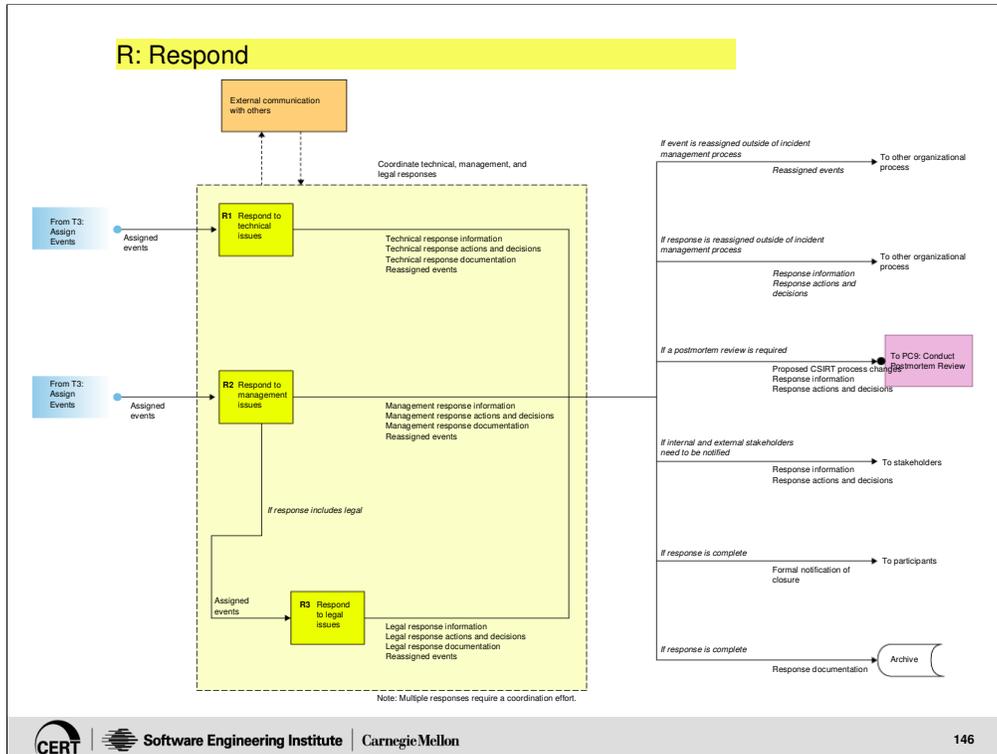
The Respond process includes the steps taken to address, resolve, or mitigate an event or incident.

We have defined three types of response activities:

- technical
- management
- legal



These three types of activities can happen simultaneously, but for the most effective response, they should happen in a coordinated function with members from all response areas coordinating the planning and execution of the response activities. Where possible and appropriate, information should be shared across these subprocesses and perhaps even with others, as needed.



In the Respond process, to maximize efficiency and effectiveness, coordination should occur across all three areas of the Respond process. All those involved in the response must communicate the steps that are being taken and any relevant information. During a particular type of response—a technical response (T1), for example—management (R2) may need to be involved before any type of legal (R3) staff are involved. This type of cooperation and coordination should occur through established communication channels that are defined in appropriate policies, procedures, and plans associated with the Respond process.

Actions must be coordinated to ensure that duplicate effort does not occur and that all tasks are completed within agreed-upon timeframes.

In some cases, all three processes will be initiated to resolve an incident, while for others, only one or two of the processes will be required. However, regardless of which groups are activated, some type of leader or project coordinator for the overall Respond process is needed to ensure that all the appropriate tasks are being performed across all the response actors.

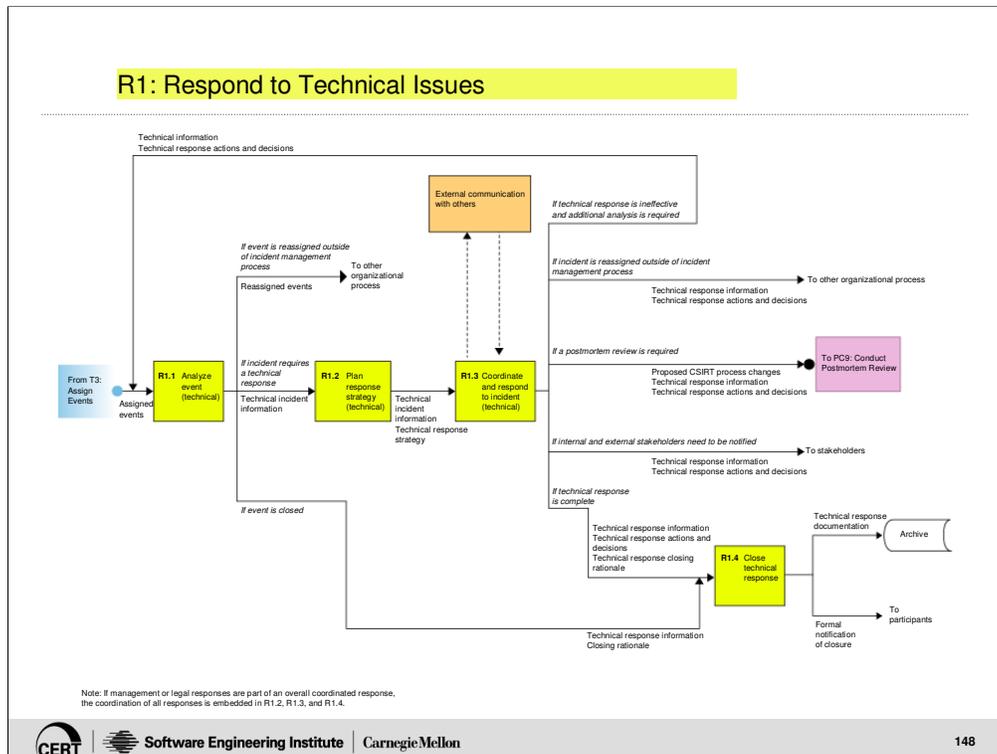
What Occurs During the Respond Process?

Actions can include

- analyzing the event
 - incident analysis
 - vulnerability analysis
 - artifact analysis
 - malicious code analysis
 - computer forensic analysis
 - business impact analysis
 - risk analysis
- planning the response strategy
 - determining what steps to take
 - identifying who will need to be involved in the response and contacting them
- coordinating efforts and responding to events or incidents
 - containing and eradicating malicious activity or threats
 - developing and disseminating alerts or notifications
 - making changes in the infrastructure
 - recovering systems and resolving the incident
- communicating with external contacts
- closing response



R1: Respond to Technical Issues



In this subprocess workflow, the response focuses on the actions taken by the technical staff to analyze and resolve an event or incident. Technical staff can include CSIRT staff such as incident, artifact, and vulnerability handlers, as well as other technical staff internal and external to the organization, such as system and network administrators, other members of IT operations, external security experts, or members of other CSIRTs as appropriate. Technical response actions can include

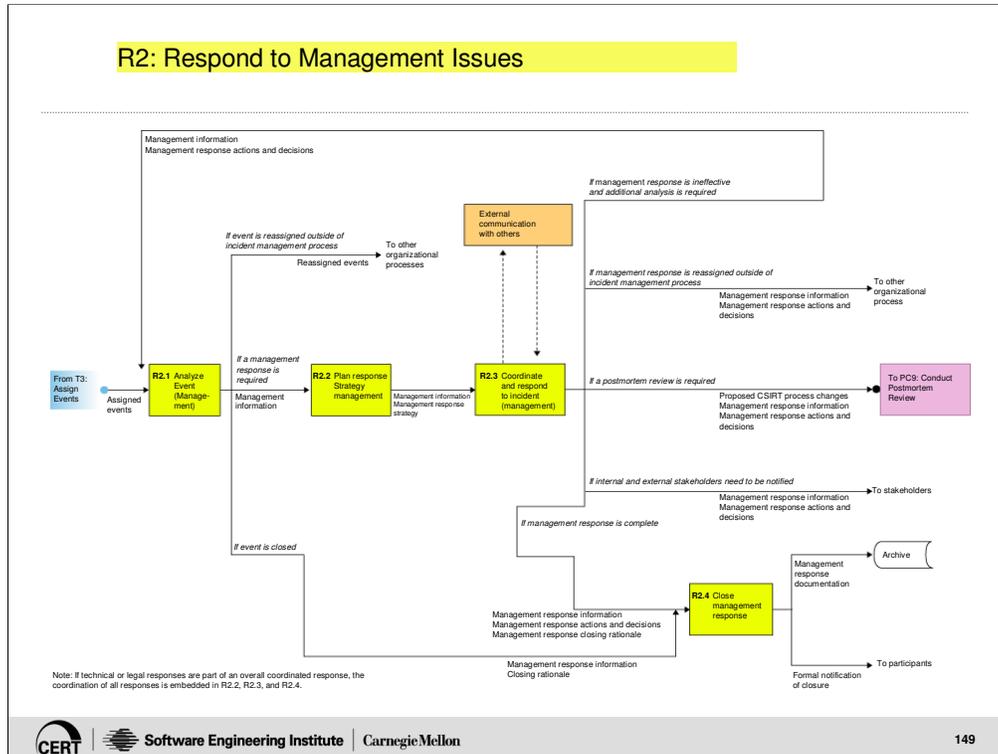
- analyzing the event or incident information, data, and supplemental material such as log files, malicious code, or other artifacts
- collecting data or other artifacts for further analysis
- researching corresponding mitigation strategies and recovery options
- developing advisories, alerts, and other publications that provide guidance and advice for resolving or mitigating the event or incident
- containing any ongoing malicious activity by making technical changes to the infrastructure, such as disconnecting affected systems from the network, changing security configurations, or filtering ports, services, IP addresses, or packet content via firewalls, mail servers, routers, or other devices
- eradicating or cleaning up any malicious processes and files
- repairing or recovering affected systems

In accordance with your CSIRT SOPs, technical response can include identifying the options available to the site such as

- who to contact
- how to recover from the incident
- how to protect against future occurrences
- which security best practices need implemented

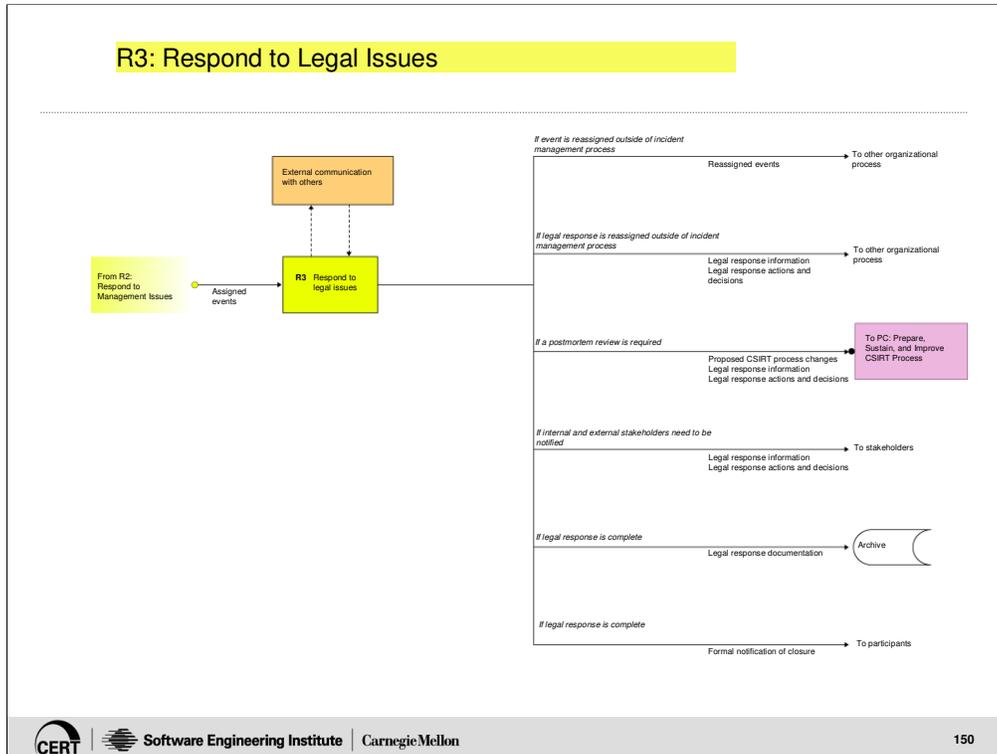
It may also include helping the site determine how the compromise took place.

R2: Respond to Management Issues



Management response highlights activities that require some type of supervisory or management intervention, notification, interaction, escalation, or approval as part of any response that is undertaken. Such management involvement may include actions taken by executive management or functional managers. Administrative or management support activities are also included in management response. These include areas of an organization such as human resources, public relations, financial accounting, audits and compliance, and other internal organizational entities.

Management response activities might include contacting legal counsel for advice regarding the liability related to an organizational network computing system being used to attack an external entity, or having human resources remove an employee found to be performing illegal activity on the organizational network. Management response can also involve ensuring that various parts of the organization work together to handle events and incidents to resolve any problems that occur between different parts of the organization (e.g., business functions units, application owners, or other cross-functional units).



Legal response includes actions associated with incident activity that relate to investigation; prosecution; liability; copyright and privacy issues; interpretation of legal rulings, laws, and regulations; non-disclosures; and other information disclosure agreements. In this base practice model, the legal response can be initiated only by management. This process has been mapped separately because it includes steps and activities that may be outside the domain and expertise of the incident management technical staff. These tasks involve activities such as legal prosecution, computer forensics, and determination of legal liability. Each of these requires skills, training, and procedures that are different from those required for other incident handling functions. Also, some legal response tasks can take longer to resolve than other incident response tasks, since they may involve court proceedings that could take months or years to complete.

At the time of the publication of SEI Technical Report CMU/SEI-2004-TR-015, Defining Incident Management Processes: A Work in Progress, we had not as yet expanded legal response into the third level. That is why it does not resemble the technical and management response workflows.

Response Depends on Your Role

Technical Response

- phone or email technical assistance
- on-site assistance
- data collection
- analysis of logs, files, or other data
- development and dissemination of
 - patches, fixes, workarounds or other solutions
 - advisories, alerts, technical documentation
- feedback to reporting site(s)

Management Response

- executive or upper management actions
- human resource actions
- media relations actions

Legal Response

- investigative assistance
- legal advice on liability
- review of contracts, SLAs and non-disclosures
- computer forensics
- contacting law enforcement
- prosecution



The appropriate response to provide will depend on your role and corresponding responsibilities.

Be careful not to take on actions which have been assigned to someone else. However, if these actions are not being done and they are crucial to the response effort, ensure that management is notified so they can ensure it does get done.

Each CSIRT provides a response

- defined by the CSIRT mission and goals
- guided by the CSIRT policy and procedures
- in conjunction with other parts of the organization according to their roles and responsibilities

How you respond will depend on

- what your role is: technical, management, or legal
- your CSIRT's standard operating procedures (SOPs)
- the type, nature and scope of the incident
- the priority of the incident
- the sites involved
- the expertise of reporter
- available resources

Depending on your role, policies and procedures, a response option may actually be no response at all.

Some response options such as computer forensics may actually occur as part of the technical and legal response.

Issues For Consideration in the Respond Process

Containment

- What are appropriate response strategies for containing incidents within your constituency's infrastructure?
- What systems can come offline? What systems cannot?
- What evidence must be preserved?

Insider threat

- What different procedures and participants will be involved to handle an incident perpetrated by an insider?

Communications

- Who needs to be notified and within what time frame?
- What is your communications plan?
- How will you communicate with them?

Coordination and collaboration

- Who else must you work with to effect a successful response?
- What role will each of you play in the response?
- Who is taking the lead?



With Whom Do You Coordinate?

Organizations may coordinate with numerous internal units, including

- upper and middle management
- business function managers
- IT and telecommunication groups
- local system and network administrators
- physical security group
- software development groups
- legal counsel
- media relations
- human resources
- internal investigative units
- audits and risk management

Commercial organizations may be legally obligated to contact their customers.

Organizations may also coordinate with external partners, collaborators, liaisons, or other contacts such as

- affiliates
- contractors
- vendors
- ISPs
- law enforcement
- government agencies
- critical infrastructure providers
- information sharing and analysis centers
- national, regional, local, or other types of CSIRTs



Who you actual coordinate with will depend on the purpose and mission of your CSIRT.

It is highly recommended that CSIRTs and other incident management capabilities develop relationships with the above mentioned internal and external groups.

Externally, a team should make sure it introduces itself and establishes contacts with

- Local law enforcement – find out how and when they should be contacted and how they want you to work with them.
- Local ISPs – especially if you need assistance in containing attacks, spam, or other activity within your constituency
- Vendors – of any critical systems, networks, or applications

Disseminating Information

Identify a variety of methods to reach a broader audience.

Think of the various media used by your constituency.

Do not forget to consider ways to communicate within your own team.

Email:

- creating and distributing alerts, bulletins, advisories
- rebroadcasting information from other teams/organizations, as appropriate.

Via CSIRT web pages

- incident or vulnerability information
- incident reporting forms
- current activity and FAQs
- technical documents
- blogs
- podcasts

Recorded messages on phone systems or SMS broadcasts

XML RSS channels or ATOM feeds

Press conferences and releases

Secure phones, faxes, intranets, extranets, or chat



You may need to use secure faxes, phones, or other secure networks to disseminate information.

When receiving or sending information related to an incident report

- Use standard email headers and signatures.
- Copy your CSIRT alias on all outgoing email for archival purposes to ensure that all email incoming/outgoing to the CSIRT can be tracked.
- Ensure any email sent to an individual account is resent to the CSIRT alias.
- Decrypt internal copies of any encrypted information.
 - These can be re-encrypted with an internal CSIRT key.
- Include all associated tracking numbers.

Information People Want to Know

- How serious is the threat?
- How much damage can be done?
- Is it global in scope?
- How does it work?
- How can you prevent it?
- How can you fix it?
- How fast is it spreading or how wide-spread is the activity?
- How does it compare to other attacks?
- Can the attacker be traced?
- Where was it first reported from?
- Who is affected?
- What systems are vulnerable or affected?
- Where do I go for help?
- What resources are available?
- What software versions or OS versions are vulnerable or affected?
- How many reports have been received?
- How much damage has been reported?
- What's the estimated cost of the activity?
- How to report activity or vulnerable systems?



Many of these questions can be answered during the triage process if the process is well defined and supported by effective policy, procedures, and guidance.

Documenting Response

Ensure information that is collected and actions taken or to be taken as part of the response are recorded.

This can include

- analysis done
- interviews and discussion completed
- technical, management, and legal response steps taken and rationale
- action items to be completed



Your CSIRT SOP should identify

- what information should be collected
- how incidents should be recorded and tracked

Keep the information up to date to facilitate

- determining the current work load
- correlating incident activity reports
- prioritizing incidents and action items
- handing off the incident to someone else
- providing status updates to management
- preparing for possible legal action

Closing an Incident

Inform involved parties when you close an incident.

At what point do you determine an incident closed?

- once further technical assistance or action is no longer needed.
- sites may consider an incident closed once they recover and secure their systems or see no further activity.
- even after a CSIRT and sites consider the incident closed, law enforcement may still consider the incident open or active.



How do you inform other parties (sites, CSIRTs, etc.) when closing an incident?

CERT/CC sets expectations via

- responder message on cert@cert.org alias
- wording in CERT/CC IRF
- explicit expectation setting in direct conversations or correspondence with other parties during phone calls or incident email

Best Practices

Information learned during the handling of an incident can be used to improve your protection strategies and your response process.

The respond and other incident management processes can be improved by

- conducting a postmortem review
- conducting mock operational exercises
- performing correlation and trending activities



Conducting a Postmortem Review

Conduct a formal or informal postmortem review

Build into your incident management processes postmortem reviews

- to determine lessons learned from a response
- to identify whether any improvements need to be implemented.



Inputs to the postmortem include

- proposed CSIRT process changes
- response information (information about the event or activity that was reported or passed onto the Respond process from Triage.)
- response actions and decisions (steps taken to determine, plan, and coordinate the response activities)

Outputs from the postmortem include

- recommended CSIRT process improvements
- recommended infrastructure protection changes
- lessons learned

All those involved in the respond actions should be included, as appropriate, in the postmortem review. This may include

- CSIRT staff
- CSIRT manager
- IT staff
- IT manager
- CSIRT constituent members
- business function managers (system owners/operators)
- representatives from administrative and management operations (legal, HR, PR, senior management)
- auditors, risk management staff, or compliance staff
- third parties (e.g., service providers, contractors, law enforcement)

Conducting Operational Exercises

How do you test that your incident management processes work correctly?

- mock incidents – test out situations that have not yet occurred
- table top exercises – can even be part of your staff meeting
- cyber challenges – capstone exercises within your constituency



Trends and Reports

Various types of analysis can be done across network traffic, incidents and vulnerabilities that have been handled?

- trend
- correlation
- fusion
- historical

Various reports can be created from such information.

- Some teams have worked with law enforcement to research and publish cybercrime reports.
- Other teams have worked with other security organizations to publish trend information.



What type of tools are best for such activities?



Summary

  Software Engineering Institute | Carnegie Mellon 162

Today's Challenges Impact CSIRTs

Less time to react

Need for quick (and accurate) notification

Tools that will automate incident handling tasks

Need for effective methods to collaborate and share appropriate information

Need for efficient mechanisms to triage incoming information

Requirements for policies and procedures that are established and understood



Continuous Improvement

As a new CSIRT, you will need to evaluate your progress.

- Find out what works and what does not work.
- Revise your design and implementation plans as appropriate.
- Evaluate your capabilities and services once you become operational.
- Build in feedback mechanisms to check how you are doing with your constituency, internally, and externally.

Build improvement plans based on outcomes from above activities



Once the CSIRT has been in operation, management will want to determine the effectiveness of the team.

The team will also want to ensure that it is meeting the needs of the constituency.

Evaluate Your CSIRT's Effectiveness

The CSIRT will need to develop a mechanism to evaluate the effectiveness of the CSIRT.

- This should be done in conjunction with management and the constituency.
- The results can be used to improve CSIRT processes.

Feedback mechanisms can include

- benchmarking
- general discussions with constituency representatives
- evaluation surveys distributed on a periodic basis to constituency members
- creation of a set of criteria or quality parameters that is then used by an audit or third-party group to evaluate CSIRT



Once the CSIRT has been in operation, management will want to determine the effectiveness of the team.

The team will also want to ensure that it is meeting the needs of the constituency.

Possible Performance Metrics

Information collected for comparison may include

- number of reported incidents
- response time or time-to-live of an incident
- amount of incidents successfully resolved
- amount of information reported to constituency about computer security issues or ongoing activity
- security posture of the organization
- preventative techniques and security practices in place



It may be helpful to have previously collected information on the state of the constituency or organization before the implementation of the team. This information can be used as a baseline in determining the effect of the CSIRT on the constituency.

Example: Incident Management Capability Metrics

Incident Management Capability Metrics					
{1} Major metric category					
{2} Metric subcategory					
{3} Metrics reference	{4} Metrics question				{5} Priority
{6} Not observed <input type="checkbox"/>	{7} Not applicable <input type="checkbox"/>	{8} Full	▪ statement representing full score for metric		{10} Metrics score 1.0 0.3 0.0 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
		{9} Partial	▪ statement representing partial score for metric		
Prerequisites					
▪ Controls					
▪ Activity					
Supporting Mechanisms {11} {Indicators}					
▪ Artifacts					
▪ Quality					

{12} Impact Statement					

{13} Metric References:					
{14} Regulatory References:					
{15} Guidance References:					
{16} Other Local References:					
{17} Applies to Groups:					



Metric major category and number – Protect, for example

Metric subcategory and number – Risk Assessment Support, for example

Metric reference number – represents major category, subcategory, and specific metric, e.g., 1.1.1

Metric question – the activity that is being evaluated

Priority – I through IV (where Priority I is most important)

Not Observed – used to indicate situations where metric was not observed during the evaluation

Not Applicable – In those cases where this may apply, the metric is excluded from the scoring.

Full/Full statement – statement defines what is required to rate the CSIRT as having fully met the metric

Partial/Partial statement – statement defines what is required to rate the CSIRT as having partially met the metric

Metrics score – value based on evaluation results

For Priority I metrics, the scoring selection is a “Yes” or “No”

For Priority II-IV, the scoring selections are 1.0 (Full score), 0.3 (Partial score), 0.0 (No score)

Indicators – items, actions, or criteria the evaluators can see or examine during the evaluation to help them determine whether the metric is being met (refer to additional details in guidance and scoring requirements).

Those indicators that are required for a [Full] or [Yes] score are marked with a [R]

Impact statement – a summary statement of the benefit to the organization if the incident management activity represented by the metric is performed satisfactorily

References – standards, guidelines or regulations relating to this metric, including any organizationally specific references

Applies to Groups – used to indicate the group(s) in the organization that are responsible for the activities represented by this metric. This metric would be applied to these groups during an evaluation.

CERT/CC Lessons Learned

Trustworthiness is paramount to the success of your team.

You will live or die by your credibility.

- Never violate a confidence.
- Speak only in facts.
- Don't spread rumors.
- Don't be afraid to say "I don't know."
- Set expectations repeatedly.

Be open and share sanitized information, but protect sensitive or personal information

You are generally a third party, remember your role and do not intrude in the roles of others.

Learn from others, build off their experiences.

Be aware that all CSIRTs differ.

Recognize that things take time; most CSIRTs

- have no authority over their constituency
- fail to plan for growth and are soon overwhelmed
- take 1-2 years to gain constituency recognition

If your CSIRT has no authority, learn to be effective through influence.

Train for a marathon, not a sprint.

- We will be doing this for a long time.
- Plan for the long haul.
- Leverage other resources and existing mechanisms.
- Guard against loss of focus.
- Build a network of experts who can advise and help.
- You will need endurance as well as brilliance.



Resources That Can Help

- Handbook for CSIRTs, Second Edition
<http://www.cert.org/archive/pdf/csirt-handbook.pdf>
- Defining Incident Management Processes for CSIRTs:
A Work in Progress
<http://www.cert.org/archive/pdf/04tr015.pdf>
- Organizational Models for CSIRTs
<http://www.cert.org/archive/pdf/03hb001.pdf>
- State of the Practice of CSIRTs
<http://www.cert.org/archive/pdf/03tr001.pdf>
- Incident Management Capability Metrics, Version 0.1
<http://www.cert.org/archive/pdf/07tr008.pdf>
- Incident Management Mission Diagnostic Method, Version 1.0
<http://www.cert.org/archive/pdf/08tr007.pdf>



Additional Resources

- Forming an Incident Response Team
<http://www.auscert.org.au/render.html?it=2252&cid=1920>
- Avoiding the Trial-by-Fire Approach to Security Incidents
http://www.sei.cmu.edu/news-at-sei/columns/security_matters/1999/mar/security_matters.htm
- Site Security Handbook
<http://www.ietf.org/rfc/rfc2196.txt>
- Expectations for Computer Security Incident Response
<http://www.ietf.org/rfc/rfc2350.txt>
- Internet Security Glossary
<http://www.ietf.org/rfc/rfc2828.txt>
- Terena TF-CSIRT Guide to Setting up a CSIRT
<http://www.terena.org/activities/tf-csirt/archive/acert7.html>
- ENISA Step-by-Step Guide to Setting Up a CSIRT
http://www.enisa.europa.eu/cert_guide/downloads/CSIRT_setting_up_guide_ENISA.pdf
- GOVCERT.NL CERT-IN-A-BOX
<http://www.govcert.nl/render.html?it=69>
- Computer Security Incident Handling Guide, National Institute of Standards and Technology (NIST SP 800-61)
<http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

Contact Information

CERT CSIRT Development Team

CERT® Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

Web: <http://www.cert.org/csirts/>

Email: csirt-info@cert.org

Appendix Table of Content

Appendix A	Incident Management Mapping
Appendix B	List of CSIRT Services
Appendix C	Policies and Procedures Generic List
Appendix D	Sample CSIRT Staff Roles and Descriptions
Appendix E	Sample CSIRT Infrastructure Needs
Appendix F	Create a Basic Incident Handling Capability
Appendix G	Incident Reporting Guidelines http://www.cert.org/tech_tips/incident_reporting.html
Appendix H	Swim-Lane Example
Appendix I	Reviewing Existing CSIRTs
Appendix J	CSIRT Description for CERT Polska http://www.cert.pl/txt/rfc2350.txt
Appendix K	Organizational Models
Appendix L	Creating and Managing a CSIRT Action Plan



Appendix A

Incident Management Mapping



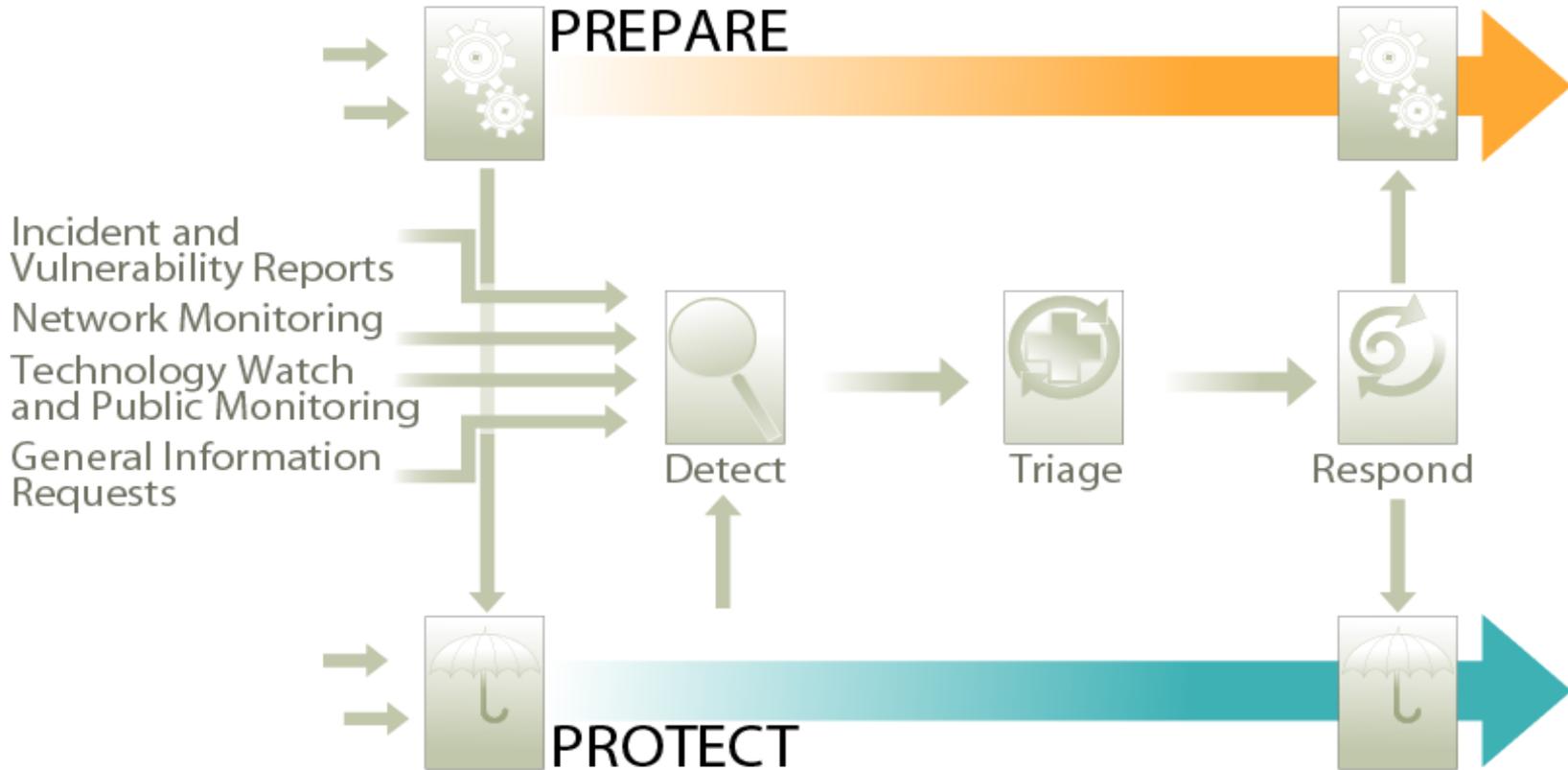


Incident Management Mapping

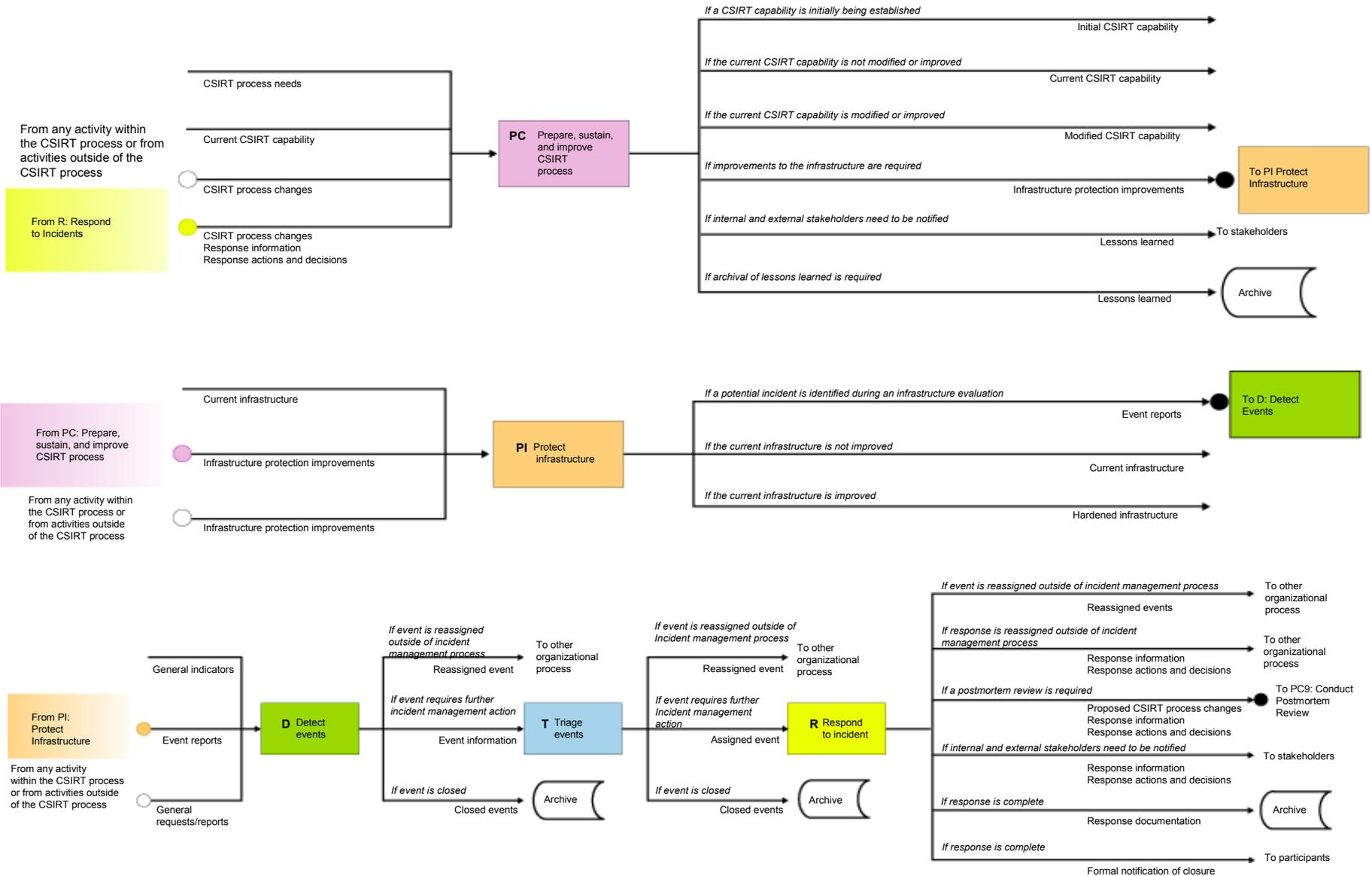
**This material is approved for public release.
Distribution is limited by the Software Engineering Institute to attendees.**



Incident Management Best Practice Model



Incident Management



PC: Prepare, Sustain, and Improve CSIRT Process

Trigger 1

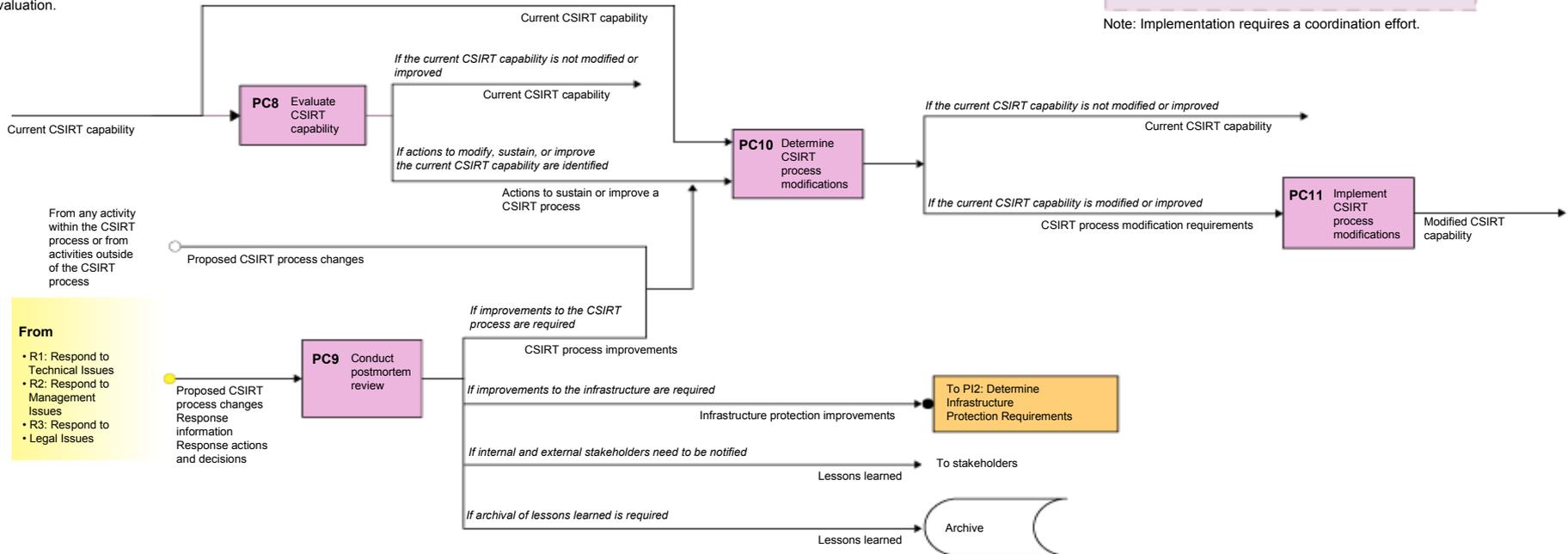
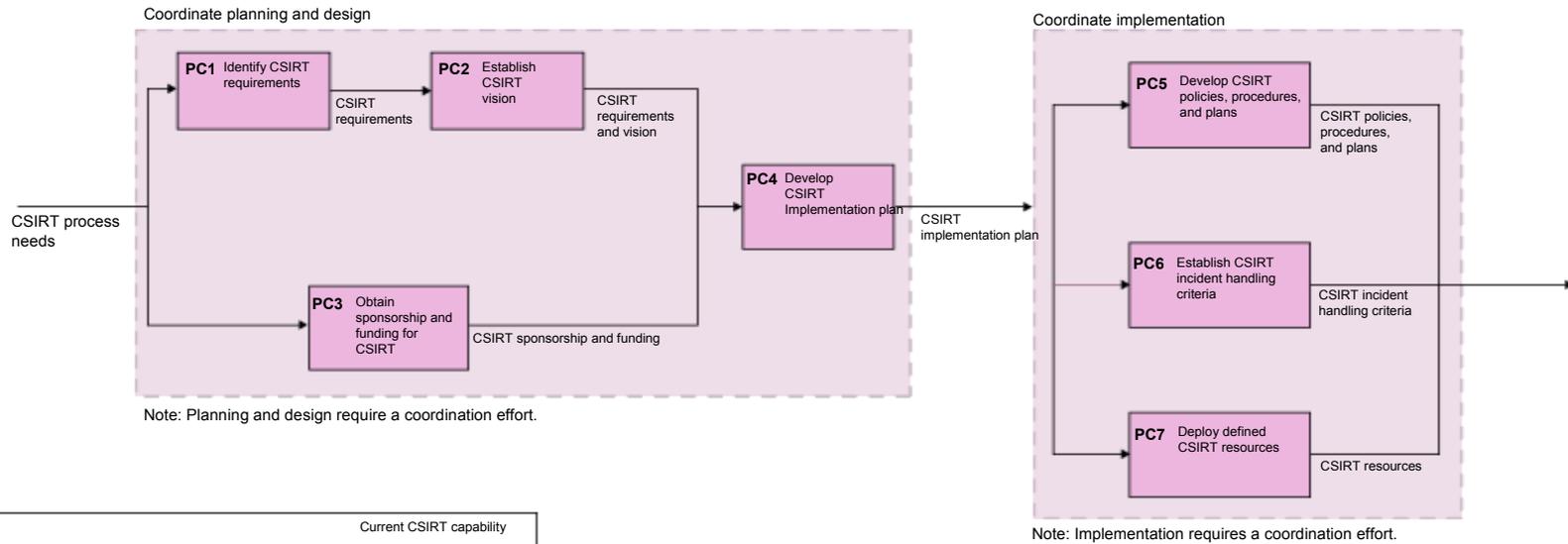
When a CSIRT capability is initially being established, Processes PC1 through PC7 are completed.

Trigger 2

When changes or improvements to an existing CSIRT capability have been identified through means other than an evaluation, Processes PC 10 and PC11 are completed. PC 9 is optional. It is completed only when a postmortem review is needed to identify CSIRT process improvements.

Trigger 3

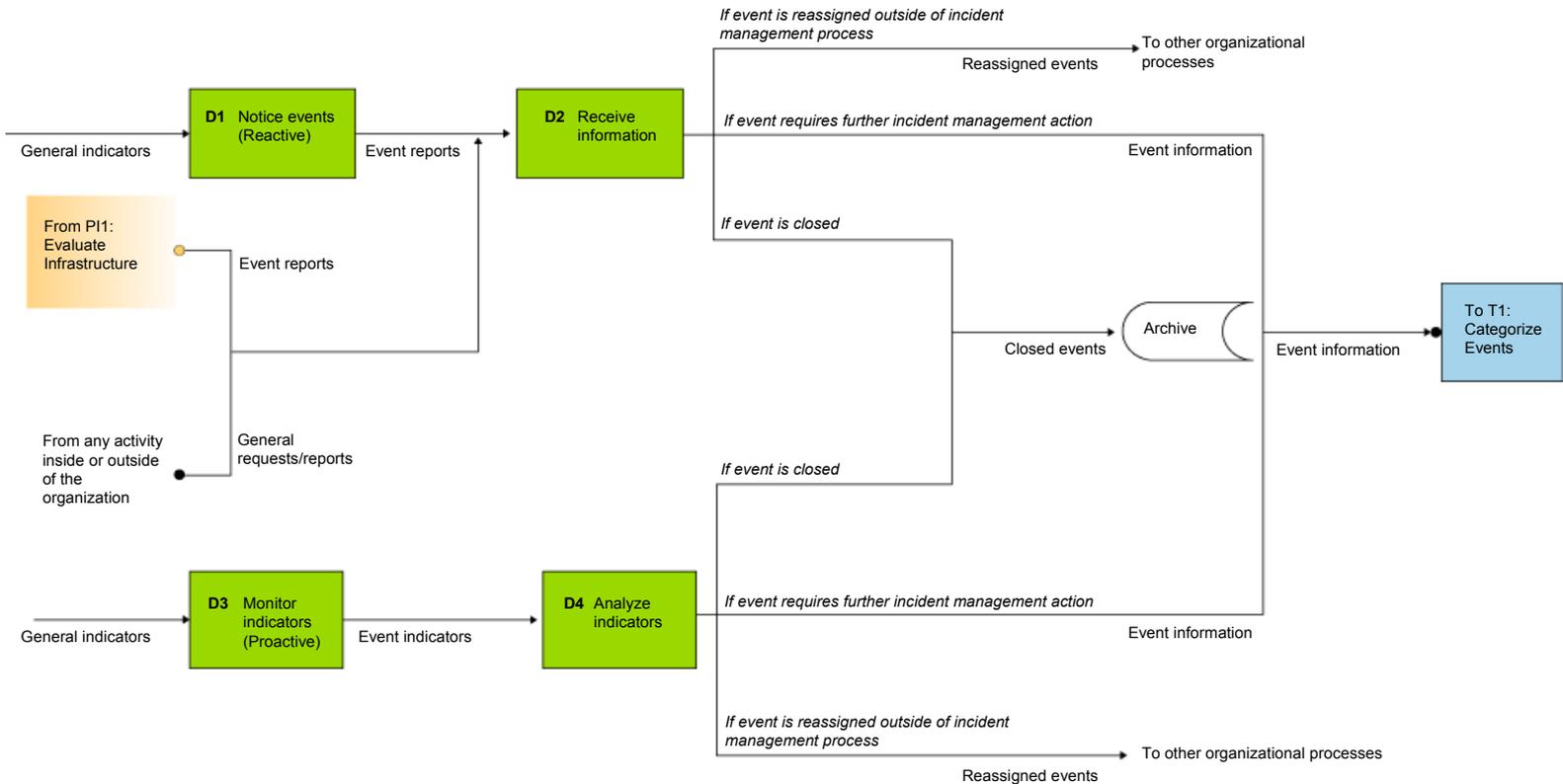
When an existing CSIRT capability is evaluated, then PC8 is conducted. PC10 and PC11 may also be completed, depending on the results of the evaluation.



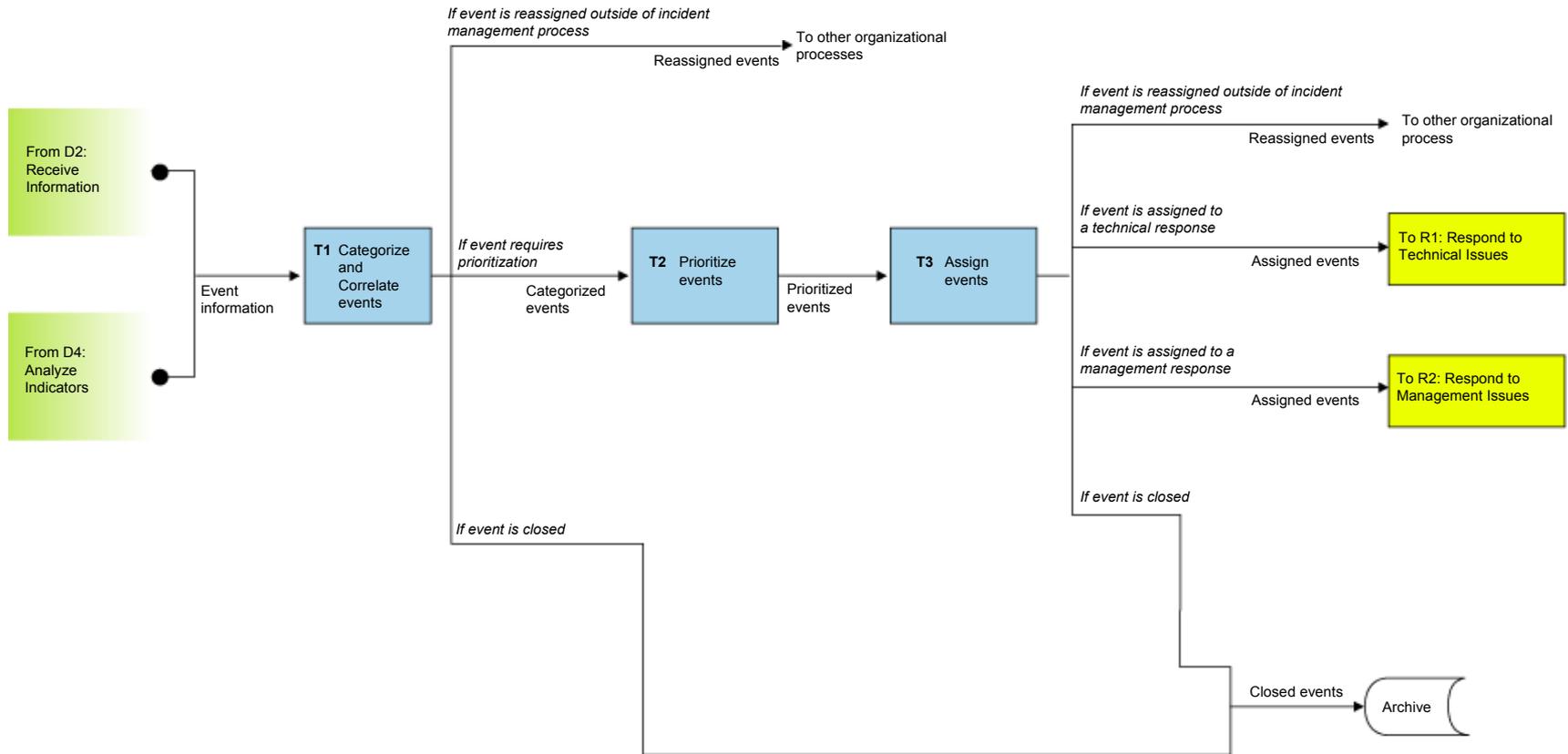
From

- R1: Respond to Technical Issues
- R2: Respond to Management Issues
- R3: Respond to Legal Issues

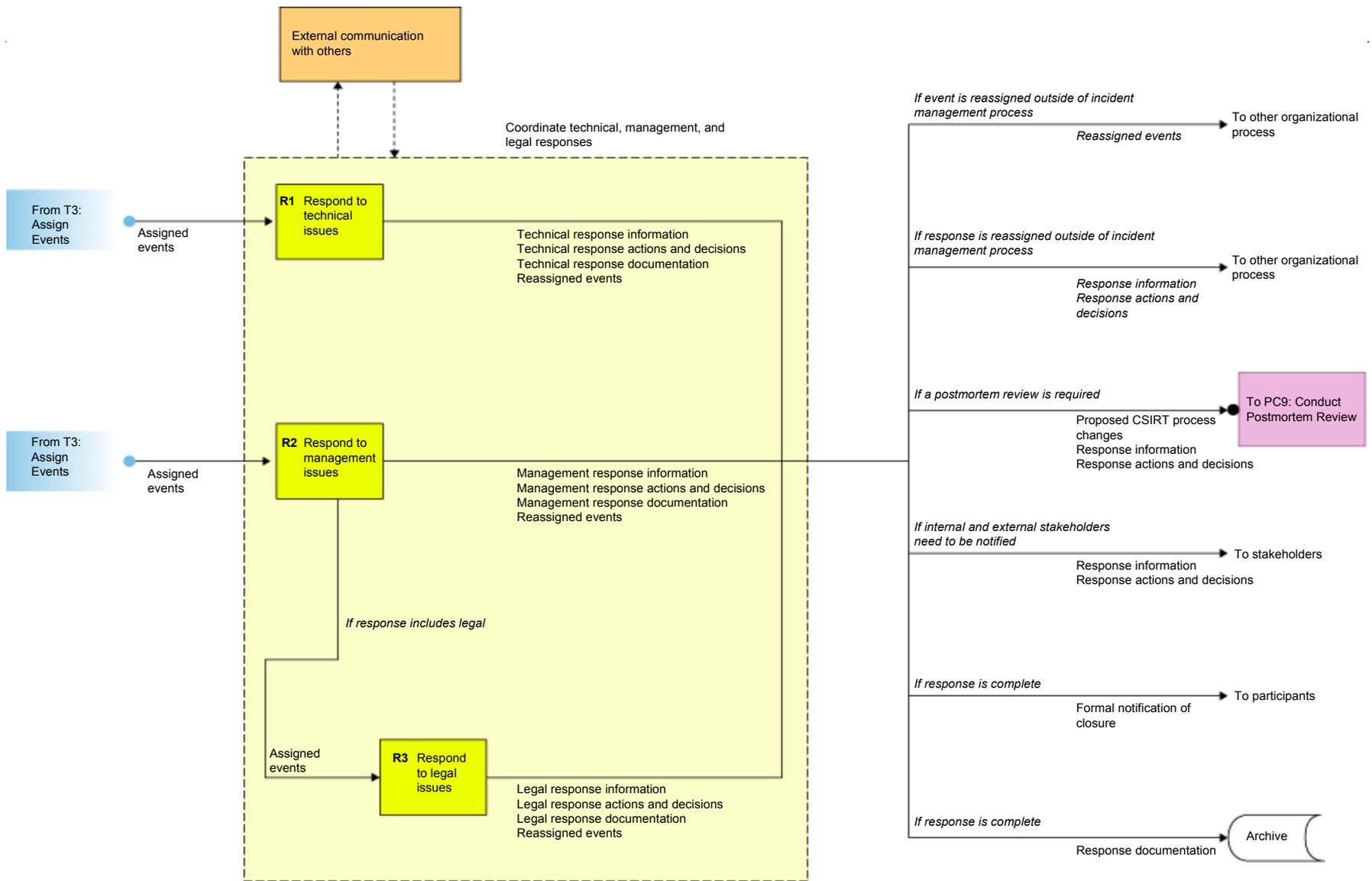
D: Detect Events



T: Triage Events

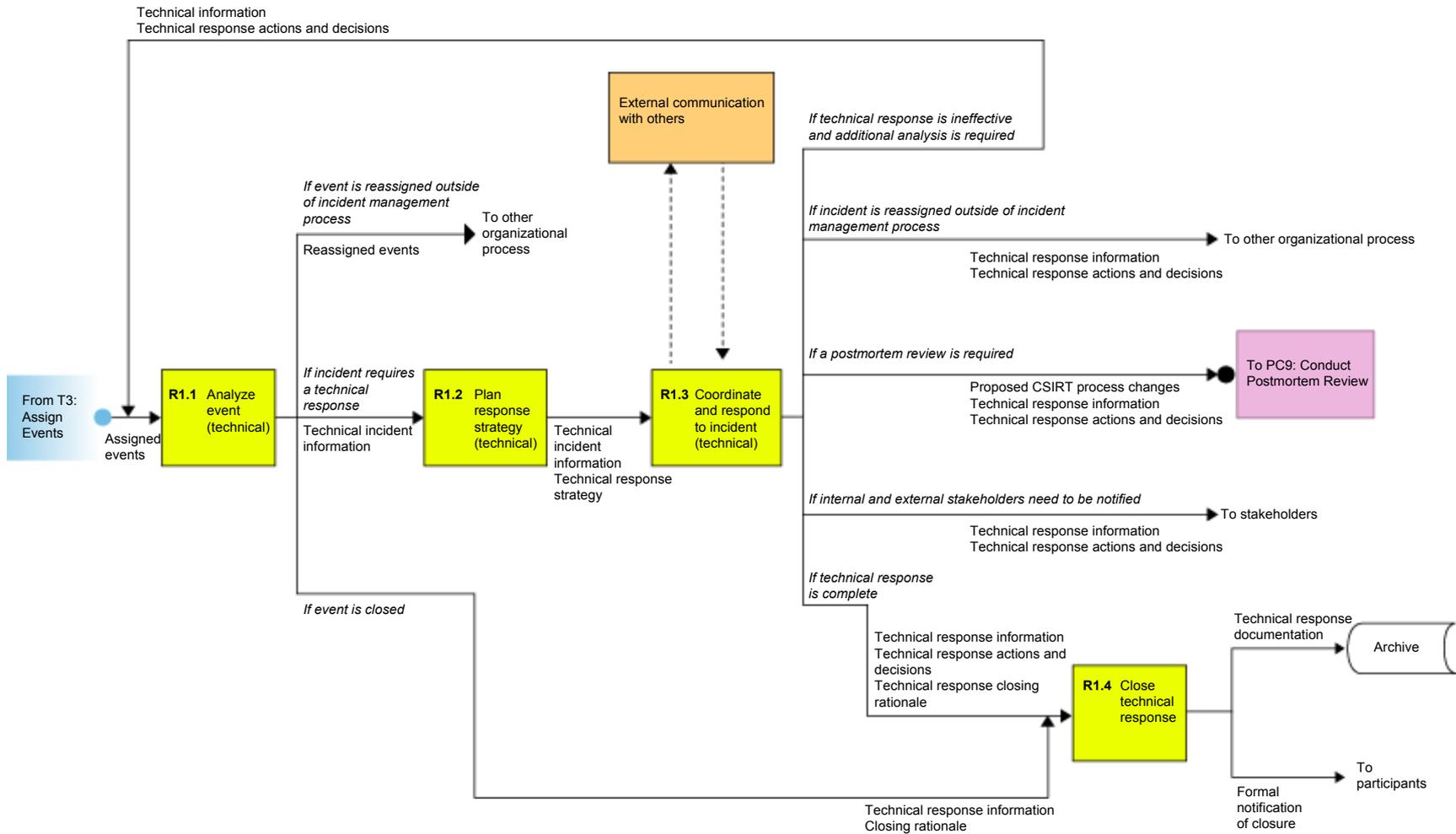


R: Respond



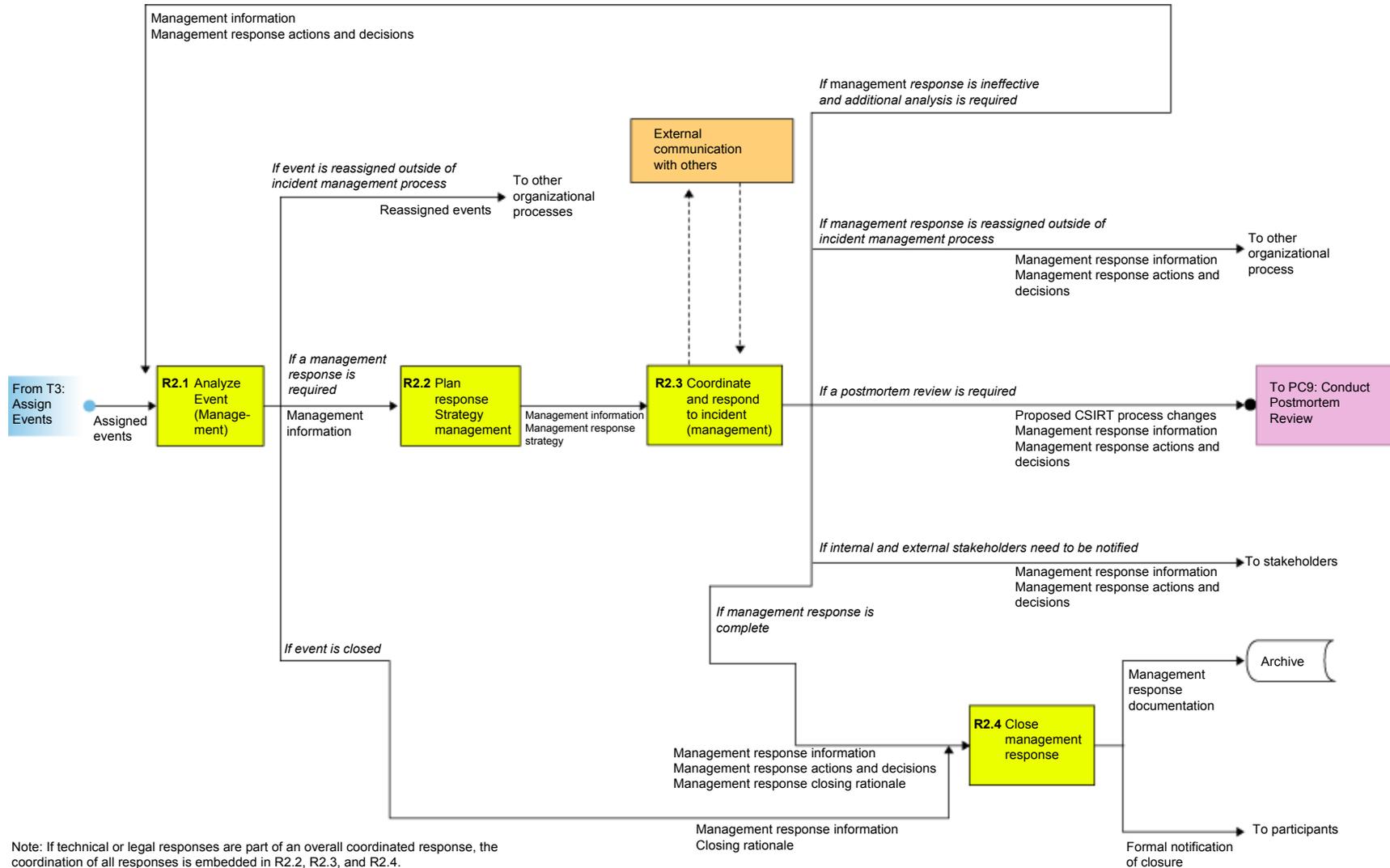
Note: Multiple responses require a coordination effort.

R1: Respond to Technical Issues

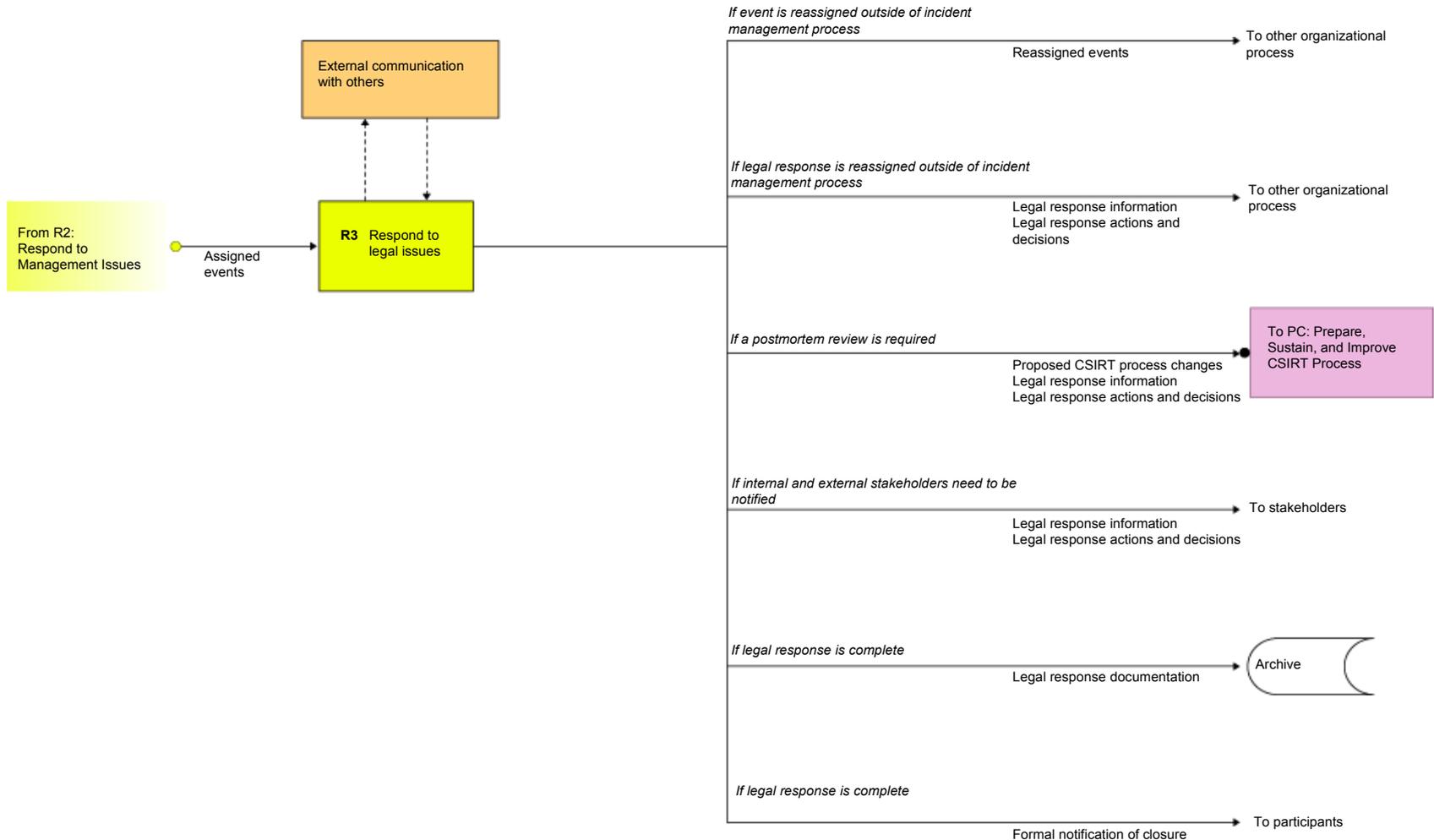


Note: If management or legal responses are part of an overall coordinated response, the coordination of all responses is embedded in R1.2, R1.3, and R1.4.

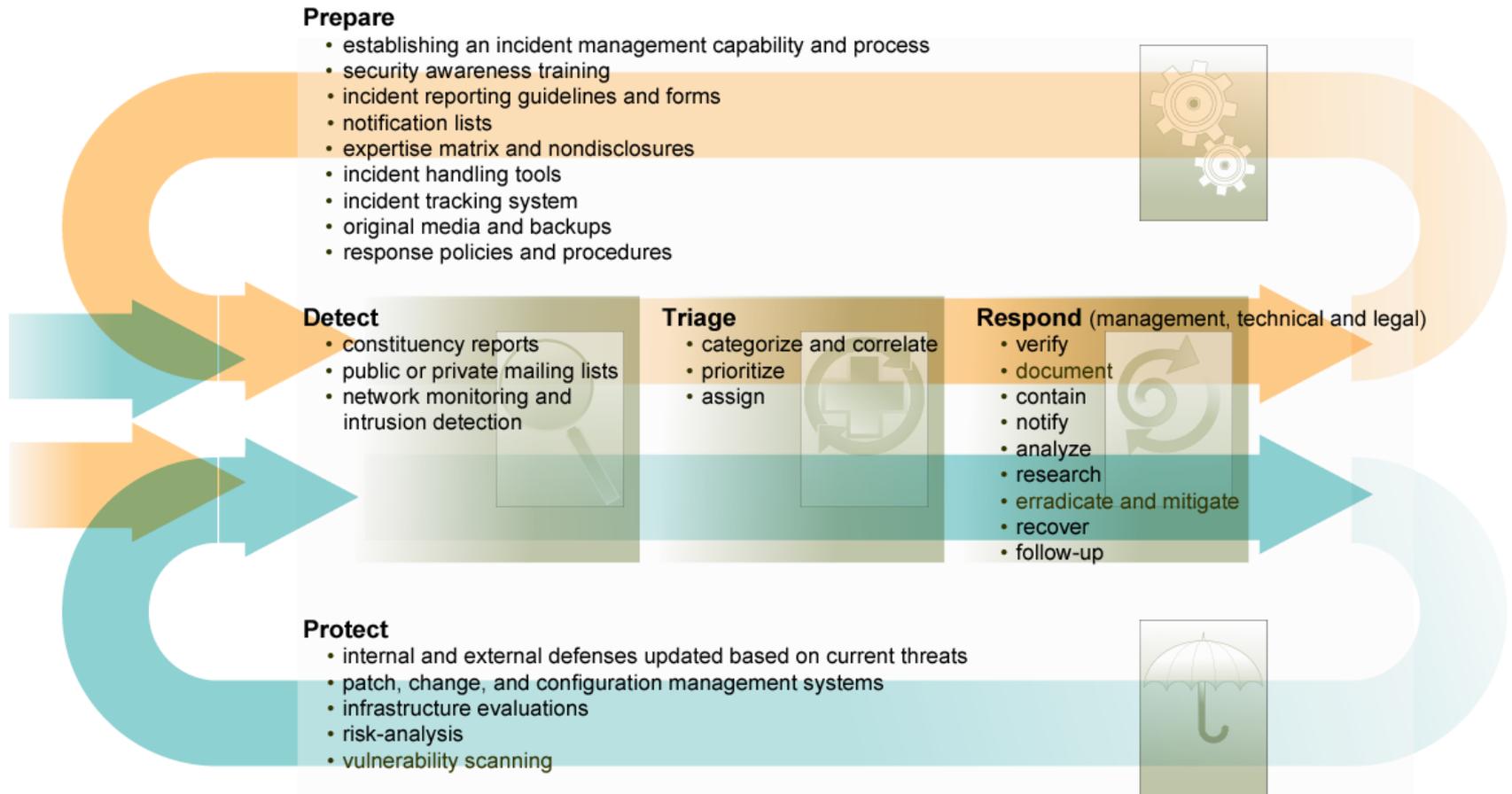
R2: Respond to Management Issues



R3: Respond to Legal Issues



Incident Response Starts Before an Incident Occurs





Appendix B

List of CSIRT Services



Appendix B: List of Services

CSIRT Services

Introduction

One of the primary issues to be addressed in creating a computer security incident response team (CSIRT) is deciding what services the CSIRT will provide to its constituency. This process also involves naming and defining each provided service, which is not always an easy task. Experience has shown that there is often great confusion about the names used for CSIRT services. The purpose of this document is to present a list of CSIRT services and their definitions.¹ This list provides a common framework for a consistent and comparable description of CSIRTs and their corresponding services.

Although this document focuses on services provided by CSIRTs, many of these same services can also be provided by system, network, and security administrators who perform ad hoc incident handling as part of their normal administrative work when there is no established CSIRT. We refer to this type of ad hoc team as a “security team.” The enclosed service definitions can also be used by any of these organizational teams or others in the computer security field.

A CSIRT must take great care in choosing the services it will offer. The set of services provided will determine the resources, skill sets, and partnerships the team will need to function properly. The selection of services should first and foremost support and enable the business goals of the CSIRT’s constituency or parent organization. The services provided should be those that the team can realistically and honestly provide based on the team size and range of expertise. It is better to offer a few services well than a large range of services poorly. As a CSIRT gains the trust and respect of its constituency, it can look to expand its services as staff and funding permit.²

Service Categories

There are many services that a CSIRT can choose to offer. Each CSIRT is different and provides services based on the mission, purpose, and constituency of the team. Providing an incident handling service is the only prerequisite to be considered a CSIRT.

¹ The list was originally based on the example CSIRT services on page 20 of the [Handbook for Computer Security Incident Response Teams \(CSIRTs\)](#) [1]. An extended and updated list was developed by Klaus-Peter Kossakowski in the book *Information Technology Incident Response Capabilities* [2]. When Kossakowski became involved with the [Trusted Introducer for CSIRTs in Europe](#) [3], the new list was utilized to help teams describe themselves based on established service names. In an effort to consolidate CSIRT service terminology, the Trusted Introducer service worked with the CSIRT Development Team of the CERT Coordination Center, Pittsburgh, PA, to produce this updated and more comprehensive list of CSIRT services.

² More information on selecting services can be found in the [Handbook for Computer Security Incident Response Teams \(CSIRTs\)](#)

CSIRT services can be grouped into three categories:

Reactive services. These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CSIRT work.

Proactive services. These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.

Security quality management services. These services augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the CSIRT performs or assists with these services, the CSIRT’s point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

The services are listed in the following table and described in detail below.

Reactive Services	Proactive Services	Security Quality Management Services
Alerts and Warnings Incident Handling Incident analysis Incident response on site Incident response support Incident response coordination Vulnerability Handling Vulnerability analysis Vulnerability response Vulnerability response coordination Artifact Handling Artifact analysis Artifact response Artifact response coordination	Announcements Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Tools, Applications, and Infrastructures Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	Risk Analysis Business Continuity and Disaster Recovery Planning Security Consulting Awareness Building Education/Training Product Evaluation or Certification

It should be noted that some services have both a reactive and proactive side. For example, vulnerability handling can be done in response to the discovery of a software vulnerability that is being actively exploited. But it can also be done proactively by reviewing and testing code to determine where vulnerabilities exist, so the problems can be fixed before they are widely known or exploited.

Service Descriptions

Reactive Services

Reactive services are designed to respond to requests for assistance, reports of incidents from the CSIRT constituency, and any threats or attacks against CSIRT systems. Some services may be initiated by third-party notification or by viewing monitoring or IDS logs and alerts.

Alerts and Warnings

This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the CSIRT or may be redistributed from vendors, other CSIRTs or security experts, or other parts of the constituency.

Incident Handling

Incident handling involves receiving, triaging³, and responding to requests and reports, and analyzing incidents and events. Particular response activities can include

- taking action to protect systems and networks affected or threatened by intruder activity
- providing solutions and mitigation strategies from relevant advisories or alerts
- looking for intruder activity on other parts of the network
- filtering network traffic
- rebuilding systems
- patching or repairing systems
- developing other response or workaround strategies

Since incident handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Incident analysis. There are many levels of incident analysis and many sub-services. Essentially, incident analysis is an examination of all available information and supporting evidence or artifacts related to an incident or event. The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. The CSIRT may use the results of vulnerability and artifact analysis (described below) to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. The CSIRT correlates activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Two sub-services that may be done as part of incident analysis, depending on the mission, goals, and processes of the CSIRT, are

³ Triage refers to the sorting, categorizing, and prioritizing of incoming incident reports or other CSIRT requests. It can be compared to triage in a hospital, where patients who need to be seen immediately are separated from those who can wait for assistance.

- **Forensic evidence collection:** the collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. This gathering of information and evidence must be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; and checking for Trojan horse programs and toolkits. CSIRT staff performing this function may also have to be prepared to act as expert witnesses in court proceedings.
- **Tracking or tracing:** the tracing of the origins of an intruder or identifying systems to which the intruder had access. This activity might involve tracking or tracing how the intruder entered the affected systems and related networks, which systems were used to gain that access, where the attack originated, and what other systems and networks were used as part of the attack. It might also involve trying to determine the identity of the intruder. This work might be done alone but usually involves working with law enforcement personnel, Internet service providers, or other involved organizations.

Incident response⁴ on site. The CSIRT provides direct, on-site assistance to help constituents recover from an incident. The CSIRT itself physically analyzes the affected systems and conducts the repair and recovery of the systems, instead of only providing incident response support by telephone or email (see below). This service involves all actions taken on a local level that are necessary if an incident is suspected or occurs. If the CSIRT is not located at the affected site, team members would travel to the site and perform the response. In other cases a local team may already be on site, providing incident response as part of its routine work. This is especially true if incident handling is provided as part of the normal job function of system, network, or security administrators in lieu of an established CSIRT.

Incident response support. The CSIRT assists and guides the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation. This can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies. It does not involve direct, on-site incident response actions as described above. The CSIRT instead provides guidance remotely so site personnel can perform the recovery themselves.

Incident response coordination. The CSIRT coordinates the response effort among parties involved in the incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as Internet service providers, other CSIRTs, and system and network administrators at the site. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. Part of the coordination work may involve notification and

⁴ Note that "incident response" is used here to describe one type of CSIRT service. When used in team names such as "Incident Response Team," the term typically has the broader meaning of incident handling.

collaboration with an organization's legal counsel, human resources or public relations departments. It would also include coordination with law enforcement. This service does not involve direct, on-site incident response.

Vulnerability Handling

Vulnerability handling involves receiving information and reports about hardware and software vulnerabilities;⁵ analyzing the nature, mechanics, and effects of the vulnerabilities; and developing response strategies for detecting and repairing the vulnerabilities. Since vulnerability handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Vulnerability analysis. The CSIRT performs technical analysis and examination of vulnerabilities in hardware or software. This includes the verification of suspected vulnerabilities and the technical examination of the hardware or software vulnerability to determine where it is located and how it can be exploited. The analysis may include reviewing source code, using a debugger to determine where the vulnerability occurs, or trying to reproduce the problem on a test system.

Vulnerability response. This service involves determining the appropriate response to mitigate or repair a vulnerability. This may involve developing or researching patches, fixes, and workarounds. It also involves notifying others of the mitigation strategy, possibly by creating and distributing advisories or alerts.⁶ This service can include performing the response by installing patches, fixes, or workarounds.

Vulnerability response coordination. The CSIRT notifies the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability. The CSIRT verifies that the vulnerability response strategy has been successfully implemented. This service can involve communicating with vendors, other CSIRTs, technical experts, constituent members, and the individuals or groups who initially discovered or reported the vulnerability. Activities include facilitating the analysis of a vulnerability or vulnerability report; coordinating the release schedules of corresponding documents, patches, or workarounds; and synthesizing technical analysis done by different parties. This service can also include maintaining a public or private archive or knowledgebase of vulnerability information and corresponding response strategies.

Artifact Handling

An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

⁵ A vulnerability is the existence of a flaw or weakness in hardware or software that can be exploited resulting in a violation of an implicit or explicit security policy.

⁶ Other CSIRTs might further redistribute these original advisories or alerts as part of their services.

Artifact handling involves receiving information about and copies of artifacts that are used in intruder attacks, reconnaissance, and other unauthorized or disruptive activities. Once received, the artifact is reviewed. This includes analyzing the nature, mechanics, version, and use of the artifacts; and developing (or suggesting) response strategies for detecting, removing, and defending against these artifacts. Since artifact handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Artifact analysis. The CSIRT performs a technical examination and analysis of any artifact found on a system. The analysis done might include identifying the file type and structure of the artifact, comparing a new artifact against existing artifacts or other versions of the same artifact to see similarities and differences, or reverse engineering or disassembling code to determine the purpose and function of the artifact.

Artifact response. This service involves determining the appropriate actions to detect and remove artifacts from a system, as well as actions to prevent artifacts from being installed. This may involve creating signatures that can be added to antivirus software or IDS.

Artifact response coordination. This service involves sharing and synthesizing analysis results and response strategies pertaining to an artifact with other researchers, CSIRTs, vendors, and other security experts. Activities include notifying others and synthesizing technical analysis from a variety of sources. Activities can also include maintaining a public or constituent archive of known artifacts and their impact and corresponding response strategies.

Proactive Services

Proactive services are designed to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur.

Announcements

This includes, but is not limited to, intrusion alerts, vulnerability warnings, and security advisories. Such announcements inform constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

Technology Watch

The CSIRT monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. Topics reviewed can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies. This service involves reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks. This can include communicating with other parties that are authorities in these fields to ensure that the best and most accurate information or interpretation is obtained. The outcome of this service might be some type of announcement, guidelines, or recommendations focused at more medium- to long-term security issues.

Security Audits or Assessments

This service provides a detailed review and analysis of an organization's security infrastructure, based on the requirements defined by the organization or by other industry standards⁷ that apply. It can also involve a review of the organizational security practices. There are many different types of audits or assessments that can be provided, including

- infrastructure review—manually reviewing the hardware and software configurations, routers, firewalls, servers, and desktop devices to ensure that they match the organizational or industry best practice security policies and standard configurations
- best practice review—interviewing employees and system and network administrators to determine if their security practices match the defined organizational security policy or some specific industry standards
- scanning—using vulnerability or virus scanners to determine which systems and networks are vulnerable
- penetration testing—testing the security of a site by purposefully attacking its systems and networks

Obtaining upper management approval is required before conducting such audits or assessments. Some of these approaches may be prohibited by organizational policy. Providing this service can include developing a common set of practices against which the tests or assessments are conducted, along with developing a required skill set or certification requirements for staff that perform the testing, assessments, audits, or reviews. This service could also be outsourced to a third part contractor or managed security service provider with the appropriate expertise in conducting audits and assessments.

Configuration and Maintenance of Security Tools, Applications, Infrastructures, and Services

This service identifies or provides appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the CSIRT constituency or the CSIRT itself. Besides providing guidance, the CSIRT may perform configuration updates and maintenance of security tools and services, such as IDS, network scanning or monitoring systems, filters, wrappers, firewalls, virtual private networks (VPN), or authentication mechanisms. The CSIRT may even provide these services as part of their main function. The CSIRT may also configure and maintain servers, desktops, laptops, personal digital assistants (PDAs), and other wireless devices according to security guidelines. This service includes escalating to management any issues or problems with configurations or the use of tools and applications that the CSIRT believes might leave a system vulnerable to attack.

⁷ Industry standards and methodologies might include Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), CCTA Risk Analysis and Management Method (CRAMM), Information Security Forum's Fundamental Information Risk Management (FIRM), Commonly Accepted Security Practices and Regulations (CASPR), Control Objectives for Information and (Related) Technology (COBIT), Methode d' Evaluation de la Vulnerabilite Residuelle des Systemes d'Informa (MELISA), ISO 13335, ISO 17799, or ISO 15408.

Development of Security Tools

This service includes the development of any new, constituent-specific tools that are required or desired by the constituency or by the CSIRT itself. This can include, for example, developing security patches for customized software used by the constituency or secured software distributions that can be used to rebuild compromised hosts. It can also include developing tools or scripts that extend the functionality of existing security tools, such as a new plug-in for a vulnerability or network scanner, scripts that facilitate the use of encryption technology, or automated patch distribution mechanisms.

Intrusion Detection Services

CSIRTs that perform this service review existing IDS logs, analyze and initiate a response for any events that meet their defined threshold, or forward any alerts according to a pre-defined service level agreement or escalation strategy. Intrusion detection and analysis of the associated security logs can be a daunting task—not only in determining where to locate the sensors in the environment, but collecting and then analyzing the large amounts of data captured. In many cases, specialized tools or expertise is required to synthesize and interpret the information to identify false alarms, attacks, or network events and to implement strategies to eliminate or minimize such events. Some organizations choose to outsource this activity to others who have more expertise in performing these services, such as managed security service providers.

Security-Related Information Dissemination

This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include

- reporting guidelines and contact information for the CSIRT
- archives of alerts, warnings, and other announcements
- documentation about current best practices
- general computer security guidance
- policies, procedures, and checklists
- patch development and distribution information
- vendor links
- current statistics and trends in incident reporting
- other information that can improve overall security practices

This information can be developed and published by the CSIRT or by another part of the organization (IT, human resources, or media relations), and can include information from external resources such as other CSIRTs, vendors, and security experts.

Security Quality Management Services

Services that fall into this category are not unique to incident handling or CSIRTs in particular. They are well-known, established services designed to improve the overall security of an organization. By leveraging the experiences gained in providing the reactive and proactive services described above, a CSIRT can bring unique perspectives to these quality management services that might not otherwise be available. These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities, and attacks. Feeding such experiences into the established traditional services (described below) as part of a security quality management process can improve the long-term security efforts in an organization.

Depending on organizational structures and responsibilities, a CSIRT may provide these services or participate as part of a larger organizational team effort.

The following descriptions explain how CSIRT expertise can benefit each of these security quality management services.

Risk Analysis

CSIRTs may be able to add value to risk analysis and assessments. This can improve the organization's ability to assess real threats, to provide realistic qualitative and quantitative assessments of the risks to information assets, and to evaluate protection and response strategies. CSIRTs performing this service would conduct or assist with information security risk analysis activities for new systems and business processes or evaluate threats and attacks against constituent assets and systems.

Business Continuity and Disaster Recovery Planning

Based on past occurrences and future predictions of emerging incident or security trends, more and more incidents have the potential to result in serious degradation of business operations. Therefore, planning efforts should consider CSIRT experience and recommendations in determining how best to respond to such incidents to ensure the continuity of business operations. CSIRTs performing this service are involved in business continuity and disaster recovery planning for events related to computer security threats and attacks.

Security Consulting

CSIRTs can be used to provide advice and guidance on the best security practices to implement for constituents' business operations. A CSIRT providing this service is involved in preparing recommendations or identifying requirements for purchasing, installing, or securing new systems, network devices, software applications, or enterprise-wide business processes. This service includes providing guidance and assistance in developing organizational or constituency security policies. It can also involve providing testimony or advice to legislative or other government bodies.

Awareness Building

CSIRTs may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organizational security policies. Increasing the general security awareness of the constituent population not only improves their understanding of security issues but also helps them perform their day-to-day operations in a more secure manner. This can reduce the occurrence of successful attacks and increase the probability that constituents will detect and report attacks, thereby decreasing recovery times and eliminating or minimizing losses.

CSIRTs performing this service seek opportunities to increase security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to organizational systems.

Education/Training

This service involves providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials. Topics might include incident reporting guidelines, appropriate response methods, incident response tools, incident prevention methods, and other information necessary to protect, detect, report, and respond to computer security incidents.

Product Evaluation or Certification

For this service, the CSIRT may conduct product evaluations on tools, applications, or other services to ensure the security of the products and their conformance to acceptable CSIRT or organizational security practices. Tools and applications reviewed can be open source or commercial products. This service can be provided as an evaluation or through a certification program, depending on the standards that are applied by the organization or by the CSIRT.

Summary

This document outlines and defines various incident handling services and several other services that can be provided by a CSIRT. Some teams may offer many services from this list; others may only be able to provide a few; still other teams may share the responsibility for providing these services with other parts of their parent or host organization, or they may outsource some services to an incident response or managed security services provider. As mentioned at the beginning of this document, to be considered a CSIRT, a team must provide one or more of the incident handling services: incident analysis, incident response on site, incident response support, or incident response coordination.

Experience has shown that whatever services a CSIRT chooses to offer, the parent organization or management must ensure that the team has the necessary resources (people, technical expertise, equipment, and infrastructure) to provide a valued service to their constituents, or the CSIRT will not be successful and their constituents will not report incidents to them.⁸

In addition, as changes occur in technology and Internet use, other services may emerge that need to be provided by CSIRTs. This list of services will therefore need to evolve and change over time.

If you have any comments on this list of CSIRT services or have suggestions for services that you think should be added, we would like to hear from you. Please send email to csirt-info@cert.org.

References

- [1] West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-98-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1998.
<http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html>.

⁸ If the CSIRT does not provide the services but outsources the activities to another organization such as a managed security services provider, it must still ensure that the same standards for staffing, equipment, and infrastructure are adhered to, in order to protect the CSIRT and organizational data and services.

- [2] Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001 (ISBN: 3-8311-0059-4).
- [3] Kossakowski, Klaus-Peter & Stikvoort, Don. "A Trusted CSIRT Introducer in Europe." Amersfoort, Netherlands: M&I/Stelvio, February, 2000.
<http://www.ti.terena.nl/process/ti-v2.pdf> (see "Appendix E, Basic Set of Information").



Appendix C

Policies and Procedures Generic List



Appendix C: Policies, Procedures, and Supporting Documents, Version 0.1

Prepare/Sustain/Improve: General

Policy and Procedures	
Topic	Sub-Topic
Official Announcement and Charter	▪
Concept of Operations Document	<ul style="list-style-type: none"> ▪ Defined Constituency ▪ Mission Statement or Charter ▪ Defined Organizational Home ▪ Defined Authority ▪ Defined Set of Services ▪ Defined Organizational Model ▪ Defined Relationships with Other Internal and External Organizations ▪ Contact Information
Site Security	▪
Evaluation of CSIRT Capability	<ul style="list-style-type: none"> ▪ Operational Exercises ▪ Assessment and Benchmarking ▪ Postmortems
Quality Assurance	▪
Information Disclosure	<ul style="list-style-type: none"> ▪ Media Relations ▪ Public and Private Communications Plans
Handling Sensitive Data	▪
Setting and Changing INFOCON Levels	▪
Standard Operating	<ul style="list-style-type: none"> ▪ Hours of Operation ▪ Roles and Responsibilities ▪ Rules of Engagement/Interfaces with Internal and External Organizations ▪ Shift Turnover and Operations Log

Supporting Documents
<ul style="list-style-type: none"> ▪ Critical Assets and Data Inventory ▪ Critical Asset Risk Analysis Results ▪ Computer Security Event and Incident Categories ▪ Computer Security Event and Incident Priorities ▪ Legal Compliance Requirements ▪ Major Event and Incident Criteria ▪ Data Classification Scheme ▪ Criteria for Contacting Law Enforcement and Other Investigative Organizations ▪ Network Topology ▪ Organization Chart ▪ Subject Matter Experts Matrix ▪ Postmortem Criteria ▪ Defined Document Types for Information Dissemination ▪ General POC List

Note: Some of the policies, procedures, and supporting documents listed in the tables throughout this document will be developed by the CSIRT while others will likely be developed by personnel from other parts of the organization.

Prepare/Sustain/Improve: Staffing

Policy and Procedures	
Topic	Sub-Topic
Human Error	▪
Staff Education and Training	<ul style="list-style-type: none"> ▪ Orientation ▪ Mentoring ▪ Security Awareness Training ▪ Professional Development
Security Clearances	▪
Surge Support and Reach Back	▪
Outsourcing	▪
Human Resources	<ul style="list-style-type: none"> ▪ Hiring ▪ Firing ▪ Evaluation ▪ Promotion ▪ Classification
Privacy	▪

Supporting Documents
<ul style="list-style-type: none"> ▪ Code of Conduct ▪ Job Descriptions ▪ Job Classification Scheme ▪ Certification Requirements ▪ Expertise Matrix ▪ Nondisclosures for Working with Subject Matter Experts ▪ Contractor SLAs, MOUs, and Other Agreements with Contractors

Prepare/Sustain/Improve: Equipment

Policy and Procedures	
Topic	Sub-Topic
Staff Acceptable Use	▪
Configuration and Maintenance of Staff Devices and Equipment	▪
Remote Access	▪
Use of Encryption	▪
Secure Communications	▪

Supporting Documents
▪

Prepare/Sustain/Improve: Infrastructure

Policy and Procedures	
Topic	Sub-Topic
Facilities Security	▪
Information Protection	▪
Information Retention and Disposal	▪
Business Resumption, Continuity of Operations, and Disaster Recovery	▪
Change Management	▪
Patch Management	▪
Configuration Management	▪
Software and Information Backup	▪

Supporting Documents
<ul style="list-style-type: none"> ▪ Network Topology and Services ▪ Criteria and Checklist for Moving to Backup Site

Protect Infrastructure

Policy and Procedures	
Topic	Sub-Topic
Risk Assessments	▪
Vulnerability Scanning	▪
Penetration Testing	▪
Tiger Teams	▪
Product Evaluation and Testing	▪

Supporting Documents
<ul style="list-style-type: none"> ▪ Criteria for Prioritizing Vulnerabilities and Other Problems Found During Evaluation Based on Business Impacts ▪ POC List for Notification and Receipt of Results and Recommendations

Note: Policies and procedures for most services listed in this table should address how to perform the service as well as how to disseminate any results and make any necessary improvements.

Detect Events

Policy and Procedures	
Topic	Sub-Topic
Receiving Event and Incident Reports or Notifications	▪
Call Handling	▪
Public Monitoring	▪
Proactive Network Monitoring	<ul style="list-style-type: none"> ▪ General Network Monitoring ▪ Netflow Analysis ▪ Anti-Virus Monitoring ▪ Spyware Monitoring ▪ Phishing Monitoring ▪ Trend Analysis

Supporting Documents
<ul style="list-style-type: none"> ▪ Event and Incident Reporting Guidelines and Forms ▪ Criteria for What Information to Capture for Incident Reporting, Public Monitoring and Network Monitoring ▪ POC List for Vendors of constituent and CSIRT Software and Hardware ▪ POC List for Defined Interfaces (if someone other than the CSIRT performs this monitoring) ▪ POC List for Dissemination of Detection Information ▪ Baseline of Normal Network Activity ▪ Criteria for Determining Severity Based on Business Impacts and Other Indicators

Triage

Policy and Procedures	
Topic	Sub-Topic
Categorizing and Correlating Events	▪
Prioritizing Events	▪
Assigning Events	▪
Escalation and Notification to Others	▪
Event and Incident Recording and Tracking	▪
Secure Storage of Reports	▪

Supporting Documents
<ul style="list-style-type: none"> ▪ Defined Event and Incident Categories and Priorities (already mentioned in General Policies and Procedures) ▪ Event and Incident Assignment Guidelines ▪ Escalation Matrix ▪ Severity Matrix

Respond

Policy and Procedures	
Topic	Sub-Topic
Verifying Events and Incidents	▪
Analyzing Events and Incidents	<ul style="list-style-type: none"> ▪ Incident Analysis ▪ Vulnerability Analysis ▪ Artifact Analysis ▪ Computer Forensic Analysis
Planning Response Strategy	<ul style="list-style-type: none"> ▪ Internal Communications ▪ Technical Response ▪ Management Response ▪ Legal Response
Coordinating and Responding to Different Categories of Incidents and Vulnerabilities	<ul style="list-style-type: none"> ▪ Development and Dissemination of Alerts, Warnings, or Advisories ▪ Incident Response ▪ Vulnerability Response ▪ Artifact Response
External Communications	<ul style="list-style-type: none"> ▪ Contacting Involved Sites ▪ Contacting Other CSIRTs or Security Experts ▪ Contacting Law Enforcement and Other Investigative Organizations ▪ Contacting Compliance Agencies ▪ FISMA Reporting
Response Follow-up or Data Calls	▪
Resolving and Closing Incidents	▪
Documenting and Archiving Actions Taken	▪

Supporting Documents
<ul style="list-style-type: none"> ▪ Criteria for Resolving and Closing Incidents ▪ POC List for Notifications



Appendix D

Sample CSIRT Staff Roles and Descriptions



Appendix D: Sample CSIRT Staff Roles and Descriptions

The following is a sample of the types of staffing, the range of positions, and the tasks for various positions that might be required for a CSIRT:

- manager or team lead
 - provides strategic direction
 - enables and facilitates work of team members
 - supervises team
 - represents CSIRT to management and others
 - interviews and hires new team members
- assistant managers, supervisors, or group leaders
 - supports strategic direction of assigned functional area
 - supports the team lead as needed
 - provides direction and mentoring to team members
 - assigns tasks and duties
 - participates in interviews with new team members
- hotline, help desk, or triage staff
 - handle main CSIRT telephone(s) for incident or security reports
 - provide initial assistance, depending on skills
 - undertake initial data entry and the sorting and prioritizing of incoming information
- incident handlers
 - undertake incident analysis, tracking, recording, and response
 - coordinate the reactive and proactive guidance that will be provided to the constituency (develop material such as documentation, checklists, best practices, and guidelines)
 - disseminate information
 - interact with the CSIRT team, external experts, and others (such as sites, media, law enforcement, or legal personnel) as appropriate, by assignment from team lead or other management staff
 - undertake technology-watch activities if assigned
 - develop appropriate training materials (for CSIRT staff and/or the constituency)
 - mentor new CSIRT staff as assigned
 - monitor intrusion detection systems, if this service is part of the CSIRT activities
 - perform penetration testing if this service is part of the CSIRT activities
 - participate in interviews with new staff members as directed
- vulnerability handlers
 - analyze, test, track and record vulnerability reports and vulnerability artifacts
 - research or develop patches and fixes as part of the vulnerability response effort
 - interact with the constituency, the CSIRT team, software application developers, external experts (CERT/CC, US CERT, vendors) and others (media, law enforcement, or legal personnel) as required
 - disseminate information on vulnerabilities and corresponding fixes, patches, or workarounds
 - undertake technology-watch activities if assigned
 - mentor new CSIRT staff as assigned
 - participate in interviews with new CSIRT staff
- technical writers
 - assist and facilitate the CSIRT in the development of publications such as advisories, best practices, or technical tips

- web developers
 - maintain CSIRT web site
 - create new content and corresponding designs for web site in conjunction with CSIRT staff
- trainers
 - develop and deliver curriculum for teaching new incident handlers within CSIRT
 - develop and deliver curriculum for constituency members
 - provide security awareness training
- network or system administrators
 - administer CSIRT equipment and peripheral devices
 - maintain the infrastructure for CSIRT products; this includes secure servers, the data repository, secure email, and any other internal systems required by the CSIRT.
- support staff
 - assist staff as needed to perform administrative support services
 - coordinate travel and conference arrangements as necessary
- platform specialists
 - assist in analysis and response efforts by providing specific expertise in supported technologies or operating systems (e.g., UNIX, Windows, mainframes, applications, databases)
 - may also perform incident handling, vulnerability handling or infrastructure tasks if needed



Appendix E

Sample CSIRT Infrastructure Needs



Appendix E: Sample CSIRT Infrastructure Needs

CSIRT staff have specialized infrastructure needs. Depending on the size and distribution of the organization these might include the following:

- Separate CSIRT infrastructure
(to protect data and limit access to CSIRT staff)
 - use firewalls
 - create separate services (email, FTP, webserver, DNS, backup, etc.)
 - limit physical access
 - create separate "DMZ" area for CSIRT use
- Specialized services
 - robust and flexible incident tracking system
 - interactive incident reporting forms (IIRF via WWW)
 - extranet for security professionals
 - secure encryption facilities for sending and receiving sensitive information (fax, email, etc.)
 - physical security (key cards, smart cards, biometric system)
- Secure hosts and network devices
 - ensure hosts and network devices are up to date with the latest security patches
 - configure hosts and network devices (routers, switches, hubs, firewalls, etc.) securely
 - limit access through ACLs on hosts and network devices
 - configure monitoring and logging facilities
 - install and monitor IDS tools
 - secure all media (floppy disks, tapes, etc.)
- Remote access
 - secure network connectivity (SSH, VPNs, etc.)
 - secure telephone (STU)
- Remote data issues
 - encrypting disks on laptops
 - secure offsite media storage
 - secure offsite media transport
- Disaster recovery, business continuity, or business resumption plans
- Required software, tools and hardware
 - up-to-date virus scanning software
 - encryption and decryption tools
 - file integrity checking tools (tripwire, MD5, etc.)
 - compression tools
 - forensic tools
 - hardware platforms to match what is used by the constituency
 - operating systems and software to match what is used by the constituency
 - network devices to match what is used by the constituency
 - security scanners (nessus, NFR, etc.)
 - protected power (UPS, power conditioner, generator)



Appendix F

Create a Basic Incident Handling Capability



Create a Basic Incident Handling Capability

(Focus on Resources: Equipment, Infrastructure, and Staffing)*

Goal: Define Basic Capability and Operations

ACQUIRE TECHNICAL STAFF

- Identify roles and responsibilities
- Identify staffing requirements
- Create job positions for positions
- Identify skill sets and training needs for job positions
- Develop training and mentoring strategy and materials for new staff
- Advertise positions
- Interview technical staff
- Hire technical staff for each position
- Provide first day knowledge and CSIRT-Speak to new hires
- Provide orientation to new staff
- Outline internal and external training plan for each staff

DEVELOP INCIDENT HANDLING AND PUBLICATION DOCUMENTATION

Create new or update existing procedures

Establish triage procedures

Develop procedure for managing incoming information (e.g., incidents, vulnerabilities, information requests)

- Identify how priorities should be managed with regard to incoming information
- Identify how items are assigned to technical staff
- Identify requirements for documenting actions taken
- Create and publish procedure based on results

Establish a hotlist (e.g., strategic partners and other high priority callers)

- Identify individuals/organizations to be included on hotlist
- Create a procedure for handling requests from individuals/organizations on list
- Create documentation of hotlist for dissemination
- Create and publish procedure for handling hotlist requests

Establish INFO item handling procedure

Develop procedure of how INFO item should be managed

- Identify scope of INFO items that require response
- Identify process for properly responding to INFO items
- Identify process for identifying and handling priority requests
- Identify requirements for documenting actions taken
- Create procedure based on results
- Publish INFO item handling procedure

Establish incident handling procedures

- Create incident handling flowchart
- Identify what incidents need to be handled
- Identify how priorities should be managed with regard to incidents

Review incident handling procedures from SEI Technical Report titled "Defining Incident Management Processes for CSIRTs: A Work in Progress"

- Review and develop procedures based on guidelines defined in sections a10-a18
- Review and develop procedures based on guidelines defined in sections d5-d10
- Review and develop procedures based on guidelines defined in sections Appendix E
- Review Chapter 3 titled "Handbook for Computer Security Incident Response Teams"

Communicate high-level incident response procedure document for release to select sponsors/partners

- Identify sponsors/partners that need to be aware of this procedure
- Draft high-level incident response procedure
- Obtain management approval to communicate procedure to select sponsors/stakeholders
- Send high-level procedure to select sponsors/partners requesting feedback
- Incorporate feedback as appropriate

Develop and communicate tactical procedures for performing incident handling

Goal: Create Basic Infrastructure
<i>Develop and Implement Necessary Infrastructure</i>
Develop infrastructure requirements
Determine internal versus external services (i.e., mail, dns, etc.)
Implement as appropriate
Firewalls and appropriate filtering
Network Monitoring
Mail system
Application servers
Other infrastructure components as required
Acquire and implement use of SSL certificate
Identify provider of SSL certificate
Purchase SSL certificate
Deploy ssl certificate on public website
Establish PGP/GPG for Team
Define policy and process for creation and expiration of PGP key
Verify key meets minimum security and compatability requirements
Create new key if current key is not acceptable for use
Ensure key is approved by management for use
Update public key servers with team key
Publish key information on public website
Obtain equipment for staff
obtain and configure staff desktops, laptops
obtain and configure phones, cell phones, pagers, PDAs, as appropriate
obtain and configure any other equipment

Goal: Create Supporting Tools for Capability

ENABLE EMAIL REPORTING

Create email alias

Assign responsibilities to monitor email alias

Establish lead to respond to coordinating response

Create mail archive that is compatible with next generation

Implement autoresponder

Configure mail service for autoresponder

Establish autoresponder message

Develop message in necessary languages

Approve autoresponder message

PGP sign autoresponder message

Develop policy for messages that require an autoresponder (e.g., exclude domains, what do you do with requests from strategic partners, etc)

Test autoresponder

Deploy autoresponder

ESTABLISH A 24x7 HOTLINE

Acquire analog phone line and number

Assign responsibility to staff that answer hotline during regular business hours

Establish procedures for answering hotline

Develop procedure for business hours calls

Develop procedure for out-of-hours calls (pre-answering service)

Identify technical staff for out-of-hours contact list

Identify management staff for out-of-hours contact list

Conduct hotline training

Create hotline training materials

Identify staff requiring training

Train staff

Establish procedures for out-of-hours (pre-answering service)

Establish process for forwarding calls to appropriate out-of-hours responder's mobile phone.

Establish out-of-hours answering service

Identify potential answering services

Select most appropriate answering service

Create procedure that answering service must follow

Implement answering service capability

Test quality of the answering service

Obtain answering services test scenarios from Damon Morda

Conduct test calls to verify proper process is being followed by answering service

Communicate necessary changes to answering service

Establish out-of-hours contact list (with answering service)

Identify rotation schedule

Communicate contact list to answering service

DEPLOY NECESSARY INFRASTRUCTURE AND TOOLS
Develop database documentation
Define the purpose and proper usage of each database
Create documentation for mail database
Create documentation for incident tracking database
Create documentation for contact database
Create documentation for any other needed database
Develop and implement necessary infrastructure for databases
Implement mail database
Design mail database
Develop mail database
Establish and implement appropriate access controls for mail database
Deploy mail database
Test mail database
Make necessary changes mail database based on testing
Implement incident tracking database
Design incident tracking database
Develop incident tracking database
Establish and implement appropriate access controls for incident tracking database
Deploy incident tracking database
Test incident tracking database
Make necessary changes to incident tracking database based on testing
Establish appropriate access controls for incident tracking database
Develop and implement other necessary tools and technologies
Triage Tools
Spam filtering
Network monitoring
Firewalls and appropriate filtering
Acquire and implement use of SSL certificate
Identify provider of SSL certificate
Purchase SSL certificate
Deploy ssl certificate on public website
Establish PGP/GPG for Team
Define policy and process for creation and expiration of PGP key
Verify key meets minimum security and compatability requirements
Create new key if current key is not acceptable for use
Ensure key is approved by management for use
Update public key servers with team key
Publish key information on public website

Goal: Communicate with Constituency

RAISE AWARENESS OF INCIDENT REPORTING CAPABILITY

Communicate incident response capability to select sponsors/partners

Identify select sponsors/partners

Inform them of incident handling capability

Communicate incident response capability publicly

Update public website

Publish procedure for reporting incidents

Publish PGP key information for sending information encrypted

Publish hotline number

Publish web form for reporting incidents

Publish how information is handled when incidents are reported

Publish the email address on the public website

**** This is not a comprehensive list, but an example.***



Appendix G

Incident Reporting Guidelines

http://www.cert.org/tech_tips/incident_reporting.html



Software Engineering Institute

| Carnegie Mellon



CERT[®] Coordination Center

Incident Reporting Guidelines

This document outlines suggested steps for reporting incidents to the CERT Coordination Center (CERT/CC). System administrators can use this information to report incidents effectively to the CERT/CC, other computer security incident response teams (CSIRT's), or other sites.

Introduction

- I. What type of activity should I report?
 - A. The CERT/CC's incident definition
 - B. The CERT/CC's incident priorities

- II. Why should I report an incident?
 - A. You may receive technical assistance.
 - B. We may be able to associate activity with other incidents.
 - C. Your report will allow us to provide better incident statistics.
 - D. Contacting others raises security awareness.
 - E. Your report helps us to provide you with better documents.
 - F. Your organization's policies may require you to report the activity.
 - G. Reporting incidents is part of being a responsible site on the Internet.

- III. Who should I report an incident to?
 - A. Your site security coordinator
 - B. Your representative CSIRT
 - C. The CERT Coordination Center
 - D. Other sites involved in the incident
 - E. Law enforcement

- IV. What should I include in my incident report?
 - A. When reporting an incident to the CERT/CC
 - B. When reporting to other sites and CSIRT's
 1. Incident reference numbers
 2. Information about how to contact you
 3. Disclosure information
 4. A summary of hosts involved
 5. A description of the activity
 6. Log extracts showing the activity
 7. Your timezone and the accuracy of your clock
 8. Clarify what you would like from the recipient

- V. How should I report an incident to the CERT/CC?
 - A. Electronic Mail
 - B. Telephone Hotline
 - C. Facsimile (FAX)
 - D. Encrypting Reports to the CERT/CC
 1. Pretty Good Privacy (PGP)
 2. Data Encryption Standard (DES)

VI. When should I report an incident?

Document revision history

I. What type of activity should I report?

What type of activity you should report, and the level of detail included in your report, depends on to whom you are reporting. Your local policies and procedures may have detailed information about what types of activity should be reported, and the appropriate person to whom you should report.

A. The CERT/CC's incident definition

The CERT Coordination Center is interested in receiving reports of security incidents involving the Internet. A good but fairly general definition of an incident is:

The act of violating an explicit or implied security policy.

Unfortunately, this definition relies on the existence of a security policy that, while generally understood, varies between organizations. We have attempted to characterize below the types of activity we believe are widely recognized as being in violation of a typical security policy. These activities include but are not limited to:

1. attempts (either failed or successful) to gain unauthorized access to a system or it's data
2. unwanted disruption or denial of service
3. the unauthorized use of a system for the processing or storage of data
4. changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

We encourage you to report any activities that you feel meet these criteria for being an incident. Note that our policy is to keep any information specific to your site confidential unless we receive your permission to release that information.

B. The CERT/CC's incident priorities

Due to limited resources and the growing number of incident reports, we may not be able to respond to every incident reported to us. We must prioritize our responses to have the greatest impact on the Internet community. The following type of reports receive the highest priority and are considered emergencies:

1. possible life-threatening activity
2. attacks on the Internet infrastructure, such as:
 - o root name servers
 - o domain name servers
 - o major archive sites
 - o network access points (NAPs)
3. widespread automated attacks against Internet sites
4. new types of attacks or new vulnerabilities

II. Why should I report an incident?

There are several reasons to report an incident to the CERT Coordination Center. We may be able to provide technical assistance in responding to the incident, or put you in touch with other sites involved in the same activity. Your reports allow us to collect and distribute better information about intruder activity through our statistics and documents. Reporting incidents to the CERT/CC and others helps to promote greater security awareness and improve the security of the Internet. Your organizational policies or local laws may require you to report the activity to us or some other CSIRT. Finally, notifying other sites of possible security intrusions is an important part of being a good Internet citizen.

A. You may receive technical assistance.

A primary part of our mission is to provide a reliable, trusted, 24-hour, single point of contact for security emergencies involving the Internet. We facilitate communication among experts working to solve security problems and serve as a central point for identifying and correcting vulnerabilities in computer systems.

When you report an incident to us, we can provide pointers to technical documents, offer suggestions on recovering the security of your systems, and share information about recent intruder activity. In our role as a coordination center, we may have access to information that is not yet widely available to assist in responding to your incident.

Unfortunately, our limited resources and the increasing number of incidents reported to us may prevent us from responding to each report individually. We must prioritize our responses to have the greatest impact on the Internet community.

B. We may be able to associate activity with other incidents.

The CERT/CC receives reports of security incidents from all over the world. In many cases, these incidents have similar characteristics or involve the same intruders. By reporting your incident, you allow us to collect information about recent activity in the intruder community as it relates to your incident. We may also be able to put you in touch with other sites who are pursuing legal actions against the intruder.

C. Your report will allow us to provide better incident statistics.

The CERT/CC collects statistics on the incidents reported to us. Your reports help identify vulnerabilities that are being actively exploited in the intruder community, provide information about the frequency of these attacks, and identify areas where greater community awareness is needed.

These [statistics](#) are made publicly available via our web page, the [CERT/CC annual report](#), and at presentations made at conferences.

D. Contacting others raises security awareness.

When you report an incident to the CERT/CC, we suggest that you contact the other sites involved in the activity, and that you include us in those messages. This benefits the other sites by alerting them to possible intruder activity on their systems. In many cases, unsuccessful probes you report may identify more serious security issues at the originating site.

Additionally, contacting other sites may help you respond to your security concerns by providing more information, a different perspective, or even by identifying the intruder.

E. Your report helps us to provide you with better documents.

The comments and suggestions that you provide while involved in the handling of an incident allows us to improve our tech tips, advisories, and other computer security publications. Your questions help us to understand what subjects require greater attention in future documents. And taken as a whole, your reports allow us to understand the current state of the computer security practice.

F. Your organization's policies may require you to report the activity.

Your organization's policies may require that you report this activity to the CERT/CC or another CSIRT. On the other hand, your policy may require that you not report or discuss this activity with anyone other than your site security coordinator. Before reporting activity to the CERT/CC or anyone else, check your local policies and procedures on how to proceed.

Local and/or federal laws may further dictate your behavior regarding the handling of computer security incidents. If you work for a public agency, you may be required to report the activity to a specific CSIRT. If your systems involve sensitive data, you may not be able to discuss the incident without permission. Before reporting activity to the CERT/CC or anyone else, check with your management and legal counsel.

G. Reporting incidents is part of being a responsible site on the Internet.

There is a strong historical precedent for communicating with other sites about security incidents. The Request for Comments document "[Guidelines for the Secure Operation of the Internet](#)" (RFC1281) reads:

The Internet is a cooperative venture. The culture and practice in the Internet is to render assistance in security matters to other sites and networks. Each site is expected to notify other sites if it detects a penetration in progress at the other sites, and all sites are expected to help one another respond to security violations. This assistance may include tracing connections, tracking violators and assisting law enforcement efforts.

III. Who should I report an incident to?

To determine who you should report a security incident to, first consult your local security policies and procedures. If the procedures do not explicitly identify who you should report an activity to, you should discuss the incident with your management and legal counsel before proceeding.

A. Your site security coordinator

Many security procedures identify a site security coordinator who serves as a central resource for handling violations of your security policies. This person may coordinate and handle all communications with other CSIRT's, law enforcement and other sites.

B. Your representative CSIRT

Many companies, universities, and countries have a computer security incident response team (CSIRT) dedicated to handling incidents involving their constituency. The Forum of Incident Response and Security Teams (FIRST) is a coalition of such CSIRT's. FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large.

More information about FIRST can be found on their web page at:

<http://www.first.org/>

To determine if your site is represented by a member of FIRST, you may want to review the [list of FIRST teams](#) which includes email addresses, telephone numbers, and brief descriptions of each team's constituency.

C. The CERT Coordination Center

The CERT Coordination Center welcomes reports from any site experiencing a computer security problem involving the Internet. We encourage you to include the CERT/CC on any messages you send to other sites or CSIRT's (within the limits of your site's security policies and procedures). This information will enable us to better meet our incident coordination objectives.

Information about how to contact the CERT/CC is available in [section V](#) of this document.

D. Other sites involved in the incident

Since intruders frequently use compromised hosts or accounts to attack other systems, we encourage you to report any intruder activity directly to the registered point of contact(s) of the originating host. They may be unaware of the activity involving their systems, and your note will provide the incentive to check for signs of intrusion.

We would appreciate being included on the "Cc:" line of any messages you may send to other sites regarding intruder activity.

Information about finding contact information for sites involved in incidents is available at:

http://www.cert.org/tech_tips/finding_site_contacts.html

E. Law enforcement

The CERT Coordination Center is not an investigative or law enforcement agency. We do not investigate (or maintain or disclose information about) individual intruders, and we do not conduct criminal investigations. Our activities focus on providing technical assistance and facilitating communications in response to computer security incidents involving hosts on the Internet.

If you are interested in contacting law enforcement to conduct a legal investigation, we encourage you review your local policies and procedures for guidance on how to proceed. We also encourage you to discuss the intruder's activity with your management and legal counsel before contacting law enforcement. Your legal counsel can provide you with legal options and courses of action based on your or your organization's needs. We do not have legal expertise and cannot offer legal advice or opinions.

U.S. sites interested in an investigation can contact their local Federal Bureau of Investigation (FBI) field office. To find contact information for your local FBI field office, please consult your local telephone directory or see the FBI's contact web page, available at:

<http://www.fbi.gov/contact/fo/fo.htm>

U.S. sites and foreign locations involving U.S. assets, interested in an investigation can contact their local U.S. Secret Service (USSS) Field Office. To find contact information for your local USSS Field Office, please consult your local telephone directory or see the USSS web site available at:

http://www.secretservice.gov/field_offices.shtml

To contact the USSS Electronic Crimes Branch please call:

Phone: +1(202)406-5850

Fax: +1(202)406-9233

Department of Defense Contractors, Department of Defense Entities and U.S. Military Services sites that are interested in an investigation of crimes involving the Internet, can contact the United States Department of Defense Criminal Investigative Service (DCIS), Pittsburgh, Pennsylvania at telephone number +1(412)395-6931. For information regarding DCIS please see:

<http://www.dodig.osd.mil/INV/DCIS/programs.htm>

Sites in other countries may want to discuss the activity with their local law enforcement agency to determine the appropriate steps that should be taken with regard to pursuing an investigation.

IV. What should I include in my incident report?

When reporting intruder activity, it is important to ensure that you provide enough information for the other site or CSIRT to be able to understand and respond to your report.

A. When reporting an incident to the CERT/CC:

The CERT Coordination Center has developed an Incident Reporting Form (IRF) designed to assist you in reporting an incident. This form is available at:

<https://irf.cc.cert.org/>

or

https://www.cert.org/reporting/incident_form.txt

This form prompts for all of the information discussed below in an organized manner. Completing the form may help you have a more complete understanding of the intruder's activity, even if you do not send it to the CERT/CC.

Many of the questions are optional, but having the answers to all the questions enables us to provide the best assistance. Completing the form can also help avoid delays introduced when we request the additional information needed to assist you.

The CERT/CC IRF is not intended for reporting activity to other sites or CSIRT's. Some of the information requested on the form may be sensitive in nature and is requested for the CERT/CC's internal use only. Note that our policy is to keep any information specific to your site confidential unless we receive your permission to release that information.

Some CSIRT's have adapted the CERT/CC IRF for use within their constituency. Before reporting activity to another CSIRT, we encourage you to see if they provide a similar incident reporting form.

B. When reporting to other sites and CSIRT's:

1. Incident reference numbers

The CERT/CC and many other CSIRT's assign incident reference numbers (e.g. CERT#XXXX) to reported activity. These numbers help us to track correspondence and identify related activity. Please be sure to include all incident reference numbers that have been assigned to the incident, either by the CERT/CC or other CSIRT's.

Each CSIRT has their own procedures regarding the assignment of incident tracking numbers. The CERT/CC attempts to assign a single number to all activity involving one intruder. Each number is unique and randomly selected. We

encourage you to reference this number when corresponding with other sites or CSIRT's that are involved in the incident.

When reporting activity that may be the work of multiple intruders, we request that you report each incident separately. (A common example would be two probes originating from different sites, with no other indications that the probes are related.)

Most CSIRT's, including the CERT/CC, request that the incident reference number be clearly displayed in the "Subject:" line of any mail messages regarding the incident.

2. Information about how to contact you

When contacting other sites, remember that they may not be able to contact you as easily as you might think. Perhaps they disconnected from the Internet immediately after you alerted them to the intruder's activity, and are now unable to respond to your email message. Also, some companies limit long distance or international dialing from company telephones.

To ensure that other are able to respond, provide as much contact information as you are willing to disclose. In most cases, this should include at least an email address and a telephone number. You may also wish to include a pager number, a fax number, or even a cellular telephone number. A traditional mail address may help the other site understand where you are located geographically.

It is also a good idea to specify an alternate contact at your site in case you are unavailable. Similar contact information should be provided for the alternate contact.

3. Disclosure information

The CERT Coordination Center's policy is to not release any information about a site's involvement in an incident, without the site's explicit permission to do so. While this policy ensures that you can report intruder activity to us in confidence, it also hinders our ability to put you in contact with other sites involved in the incident.

If we are authorized to offer information about your involvement in an incident to the other sites involved, other CSIRT's, or law enforcement, please state this clearly in the incident report.

Most CSIRT's have non-disclosure policies, and many sites will respect your non-disclosure requests as well. In general, a short statement describing your concerns (or lack thereof) should be included in any incident report to help the recipient understand and respect your wishes. Keep in mind however, that there is no way to ensure that other sites involved in the activity will comply with your request.

4. A summary of hosts involved

In many incidents, the most obvious indication of related activity is the hosts involved. For example, several of the hosts used to attack your site may have been used to attack another compromised host last week. For this reason, it is a good idea to include a brief summary of the hostnames and IP addresses known to be involved and their relationship to the incident.

However, you may want to exercise caution in identifying compromised hosts at your site, particularly before recovering the security of these systems. Your policies and procedures for handling computer security incidents may specify how much information you are able to release about the hosts involved at your site.

5. A description of the activity

One of the most important parts of any incident report is a description of the intruder's activity. Mention any vulnerabilities which were exploited, modifications that were made to the system, or software that was installed.

When reporting to a CSIRT, this information will allow the incident handler to provide assistance specific to the activity at your site. When reporting to another site, it helps the recipient understand what kind of intruder activity to look for on their systems.

When describing intruder activity, it is important to remember that other administrators may have more or less experience with computer security. You may want to include references to advisories or other documents which describe the activity in more detail.

6. Log extracts showing the activity

Whenever possible, you should include log entries showing the activity with your report, particularly when the logs provide significantly more detail than your description. Log entries may also be more easily understood by sites that do not speak your language fluently.

Log entries that are not related to the intruder activity should be removed to help avoid confusion. What you immediately recognize as normal entries may appear to be intruder activity to someone else.

If the intruder's activity generated a large number of very similar entries, it is usually sufficient to extract a sample portion of the log, and indicate this in the message. A quick estimate of the number of log entries is useful as well.

A description of the log format may also be helpful to system administrators who are not familiar with the logs provided. This is very important for log entries that do not include descriptive text, or are generated by tools that are not widely distributed.

When sending log entries to other sites, take care to ensure that you do not violate any non-disclosure policies you may have. Sensitive information can be removed by replacing it with X's. You may want to make a note of this in your report to ensure that the other site is aware of the changes.

If you do not have logs showing the intruder's activity (perhaps because they were deleted by the intruder), then state this clearly in your report to help minimize requests for this information.

Even if you do not include log entries showing the activity, we encourage you to describe the date and time when the events occurred. This allows the other site to review their logs when looking for related activity at their site.

7. Your timezone and the accuracy of your clock

Since the recipient may be in a different time zone, you should clearly identify the time zone for your comments and logs. A timezone reference relative to GMT (or UTC) such as GMT-5 is preferred, since less formal timezone designations can be mis-interpreted. For example, EST (Eastern Standard Time) may have different meanings for people inside and outside the United States.

If the times recorded in the log entries are known to be inaccurate by more than a minute or two, you may want to include a statement warning the recipient of this inaccuracy. On the other hand, if the system was synchronized with a national time server via NTP (Network Time Protocol), then you may want to mention this as well.

Dates, times and timezones are just a few examples of several topics that can be very confusing when used casually in international communications. Danny Smith of the Australian incident response team (AUSCERT) has prepared a document for FIRST, with several suggestions on preventing confusion when communicating with sites or CSIRT's in other countries. This document is available from:

http://www.first.org/docs/international_comms.html

8. Clarify what you would like from the recipient

If you are reporting intruder activity solely for the other site's benefit, let them know that you do not expect a response from them regarding your report. If you would like them to take a specific action, such as acknowledging your message, or providing you with additional information regarding the activity, request this politely in your message.

Keep in mind that the other site's incident handling policies and procedures may prevent them from responding as you have requested. Internet service providers frequently have policies protecting the identity of their customers, and will not release this information without a subpoena.

If a site requests information or an action from you that violates your site's security policy, politely explain that you are unable to respond as they requested.

Finally, when requesting assistance from the CERT/CC or another CSIRT, remember that resource limitations may prevent them from responding as you have requested.

V. How should I report an incident to the CERT/CC?

You can report intruder activity to the CERT/CC via electronic mail, telephone hotline, or FAX machine. We encourage you to encrypt your reports to ensure your privacy, and to authenticate your identity.

A. Electronic Mail

The CERT Coordination Center's preferred mechanism for receiving incident reports is through electronic mail. Electronic mail allows us to prioritize the incidents reported to us, and to reply to those messages quickly and efficiently.

Electronic mail also provides an accurate and efficient medium for exchanging information too complex to discuss over the telephone, such as packet dumps, or large log files. Finally, e-mail provides a reliable log of communications that we may refer to in the process of responding to an incident.

Our electronic email address is: cert@cert.org.

B. Telephone Hotline

If you have disconnected from the Internet to recover from a compromise, or if you are unable to send mail due to a denial of service attack, you can contact the CERT/CC on our telephone hotline.

Our telephone hotline number is: +1 412-268-7090.

Occasionally, a compromised system's electronic mail will be monitored by the intruder. If you are unable to obtain Internet mail access from a secure system, and you do not want to alert the intruder by using e-mail on the compromised system, you may also want to contact us on the telephone.

Please keep in mind that while the CERT hotline is staffed 24 hours a day, outside of normal working hours incident handlers are available only for [emergency calls](#). Normal working hours are from 8:00am to 5:00pm EST(GMT-5)/EDT(GMT-4), Monday through Friday. Hours may vary on holidays or under other special circumstances.

C. Facsimile (FAX)

When electronic mail is not available or provides inadequate security, and you have logs or other information that is not easily conveyed on the telephone, you may want to send that information to us via FAX.

The CERT/CC FAX machine is checked regularly during normal working hours. Faxes received during the evenings, weekends, and holidays will be reviewed on the next business day.

Our FAX number is: +1 412-268-6989.

D. Encrypting Reports to the CERT/CC

Electronic mail provides little or no privacy for the information you send across the Internet. If you wish to ensure that mail sent to the CERT/CC is not read by unauthorized people while in transit, we encourage you to use a strong encryption algorithm.

The CERT Coordination Center currently supports two encryption mechanisms. The first is a public key based on the Pretty Good Privacy (PGP) product. We also support shared private keys through the Data Encryption Standard (DES).

1. Pretty Good Privacy (PGP)

PGP is the CERT/CC's preferred encryption mechanism. It provides authentication and privacy. No special arrangements have to be made with us in advance in order to communicate securely via PGP.

You can obtain our public key from our web server at:

http://www.cert.org/contact_cert/encryptmail.html

This key will allow you to ensure the privacy of messages sent to us, and verify the authenticity of messages you receive from us.

If you encrypt messages you send to the CERT/CC, we will respond with encrypted messages whenever possible. Since it can be difficult for us to confirm the validity of your public PGP key, please be sure to include your public key in the body of any encrypted messages you send to us.

The CERT/CC signs all outgoing mail with our PGP key. If you receive any communication from us without a PGP signature, or with an invalid PGP signature, please consider the message suspect, and let us know. We encourage all sites communicating with us to encrypt and sign their e-mail messages with PGP.

More information about PGP is available from:

<http://www.pgp.com/>

2. Data Encryption Standard (DES)

A shared private DES key must be established over a secure communication channel before messages can be exchanged. Please call our telephone hotline during normal business hours to establish a shared private DES key.

VI. When should I report an incident?

Incident reports that are sent shortly after the incident occurred are the most likely to be valuable to the recipient and to us. This does not imply that an incident report becomes useless after some period of time. We encourage you to report all activity you discover, even if the intruder's activity is quite old by the time you report it.

Other than being extra careful to ensure that the date of the activity is clearly identified, we encourage you to report the incident as you would any other incident, since other sites may not yet be aware of the incident.

This document is available from: http://www.cert.org/tech_tips/incident_reporting.html

CERT/CC Contact Information

Email: cert@cert.org

Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989

Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

<http://www.cert.org/>

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

[Conditions for use, disclaimers, and sponsorship information](#)

Copyright 1998, 1999, 2000, 2001 Carnegie Mellon University.

Revision History

May 11, 1998	Initial Release
Feb 12, 1999	Converted to new web format
Apr 12, 2000	Updated section on activity to report
May 24, 2000	Updated several hyperlinks
Jul 30, 2001	Updated URLs for incident reporting form



Appendix H

Swim-Lane Example



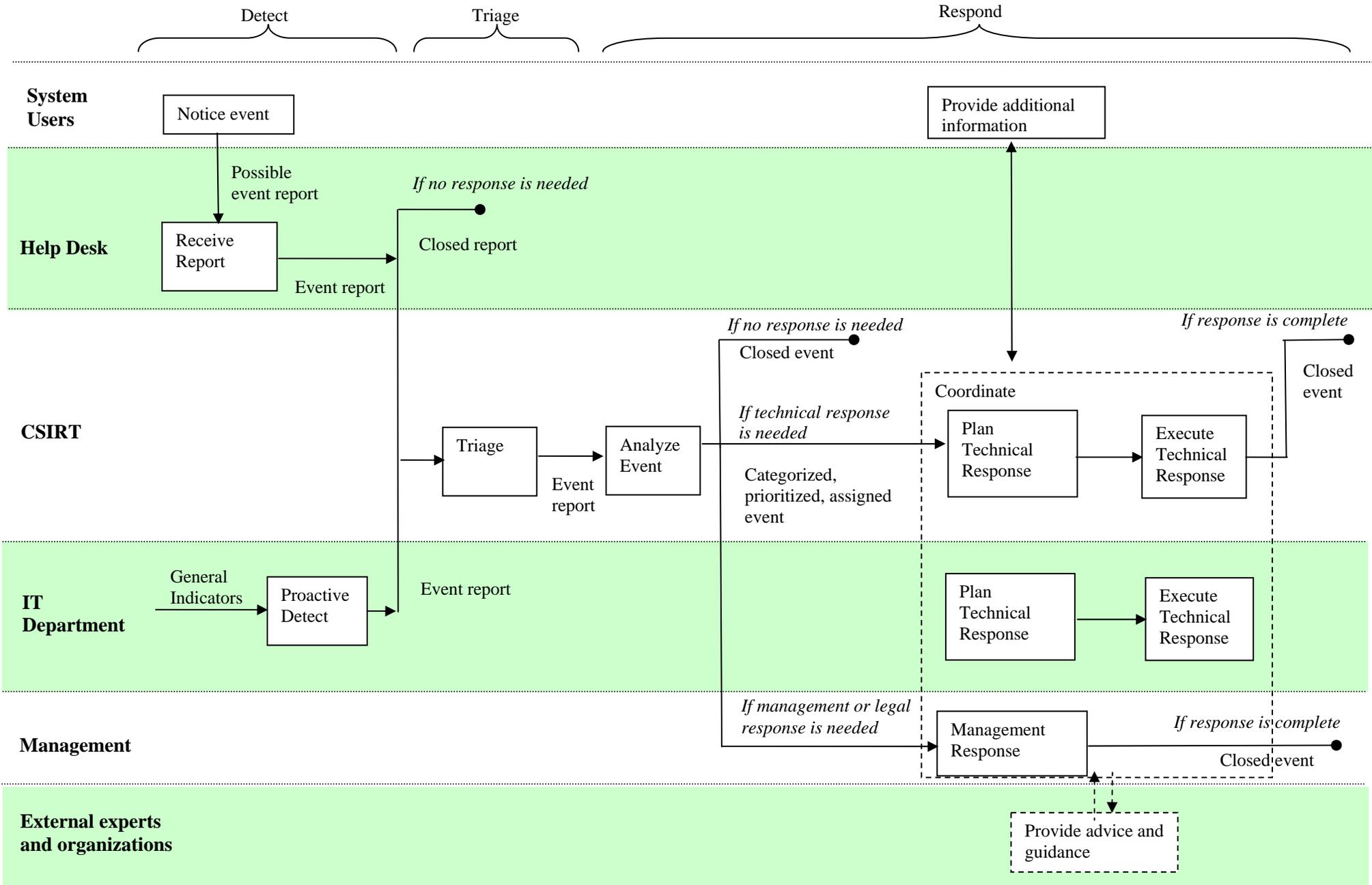


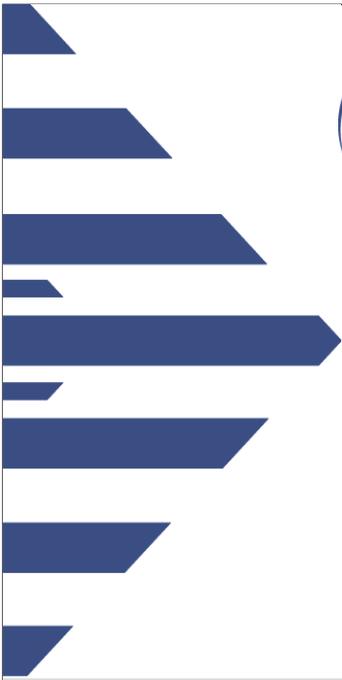
Figure 1. Example of Swim-Lane Chart Showing a Specific Instantiation of an Incident Handling Capability Derived from the Detect, Triage, and Respond Process Workflows and Descriptions



Appendix I

Reviewing Existing CSIRTs



A series of horizontal blue bars of varying lengths on the left side of the slide, with the longest bar pointing to the right towards the title.

Reviewing Existing CSIRTs

This material is approved for public release.
Distribution is limited by the Software Engineering Institute to attendees.



CERT/CC Mission Statement

“The CERT is chartered to work with the internet community in detecting and resolving computer security incidents, as well as taking steps to prevent future incidents.”

http://www.cert.org/meet_cert/meetcertcc.html#A



Additional information:

“In particular, our mission is to

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Facilitate communication among experts working to solve security problems.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Maintain close ties with research activities and conduct research to improve the security of existing systems.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.”

Source: CERT Coordination Center

http://www.cert.org/meet_cert/meetcertcc.html#A

“The CERT/CC is funded primarily by the U.S. Department of Defense and a number of Federal civil agencies. Other funding comes from the private sector. As part of the Software Engineering Institute, some funds come from the primary sponsor of the SEI, the the Office of the Under Secretary of Defense for Acquisition and Technology.”

- CERT Coordination Center
http://www.cert.org/faq/cert_faq.html#A4

CERT.br

“CERT.br, formerly known as NBSO/Brazilian CERT, is the Brazilian Computer Emergency Response Team, sponsored by the Brazilian Internet Steering Committee. CERT.br is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity related to networks connected to the Brazilian Internet.

Besides doing Incident Handling activities, CERT.br also works to increase security awareness in our community and to help new CSIRTs to establish their activities.

Our range of services include:

- Provide a focal point for reporting computer security incidents that provides coordinated support in response (and indication to others) to such reports;
- Establish collaborative relationships with other entities such as law enforcement, service providers and telecom companies;
- Support tracing intruder activity;
- Provide training in Incident Response, specially for CSIRT staff and for institutions starting the creation of a CSIRT.”

<http://www.cert.br/mission.html>



JPCERT/CC Mission Statement

“JPCERT/CC is a first CSIRT (Computer Security Incident Response Team) established in Japan. The organization coordinates with network service providers, security vendors, government agencies, as well as the industry associations. As such, it acts as a "CSIRT of the CSIRTs" in the Japanese community. In Asia Pacific region, JPCERT/CC helped form [APCERT \(Asia Pacific Computer Emergency Response Team\)](#) and provides a secretariat function for APCERT. Globally, as a member of [Forum of Incident Response and Security Teams \(FIRST\)](#), JPCERT/CC coordinates its activities with the trusted CSIRTs worldwide.”

<http://www.jpccert.or.jp/english/aboutus.html>



Japan Computer Emergency Response Team Coordination Center
<http://www.jpccert.or.jp/english/about.html>

“The Objects of JPCERT/CC

- Provide computer security incident responses;
- Coordinate with domestic and international CSIRTs and related organizations;
- Foster the establishment of a new CSIRT and collaboration among CSIRTs;
- Gather and disseminate technical information on computer security incidents and vulnerabilities and security fixes, and other security information, as well as issue alerts and warnings;
- Provide research and analysis of computer security incidents;
- Conduct research on security related technologies; and
- Increase awareness and understanding of information security and the technical knowledge through education and training.”

MyCERT Mission Statement

“To address the computer security concerns of local Internet users.”

<http://www.mycert.org.my/>



This is found on the “About Us” link on the MyCERT Homepage.

Functions:

- MyCERT provides a point of reference of expertise on network and security matters.
- MyCERT centralizes reporting of security incidents and facilitates communication to resolve security incidents.
- MyCERT disseminate security information including system vulnerabilities, defence strategies and mechanism.
- MyCERT acts as a repository of security related information, acquiring patches, tools and technique.
- MyCERT also plays an educational role in educating the public with regard to computer security in Malaysia

CanCERT™

“CanCERT™ is Canada’s first national Computer Emergency Response Team. Operated since 1998 by EWA-Canada Ltd., CanCERT™ is a trusted centre for the collection, analysis and dissemination of information related to networked computer threats, vulnerabilities, incidents and incident response for Canadian governments, businesses and academic organizations”

<http://www.cancert.ca/>



Software Engineering Institute | Carnegie Mellon

6

“Our goals are:

- To provide accurate, timely and trusted security information to the CanCERT™ client.
- To increase awareness of networked computer threats, vulnerabilities, incidents and incident responses.
- To provide advanced warning of attack via Canadian and world-wide statistics.
- To foster collaboration and the sharing of security-related information.
- To aid the CanCERT™ client in emergency incident response.
- To assist the CanCERT™ client in applying the best information technology security practices available. “

Source: <http://www.cancert.ca/>

CERT Polska

CERT Polska's goals:

- “providing a single, trusted point of contact in Poland for the NASK customers community and other networks in Poland to deal with network security incidents and their prevention
- responding to security incidents in networks connected to NASK and networks connected to other Polish providers reporting of security incidents
- providing security information and warnings of possible attacks cooperation with other incident response teams all over the world”

<http://www.cert.pl/english.html>



NASK is the Research and Academic Network in Poland.

CERT Polska is the CSIRT for NASK.

<http://www.nask.pl/>

HOUSECIRT

“The United States House of Representatives Computer Incident Response Team, established by HIR in 1996, is the single point of contact for the House for reporting and handling computer security incidents and vulnerabilities. The HOUSECIRT will coordinate the technical resources of HIR to assess, analyze, and provide countermeasures for computer security incidents and vulnerabilities reported by House computer users, security managers, and system managers.”

<http://www.house.gov/ushcert>



“The Mission of HOUSECIRT is to...

- Maintain information security by the proactive application of reasonable security "layers."
- Raise the collective information security "level of consciousness" by enacting a positive and creative security awareness program.
- Serve as the central coordination center for security information and concerns.
- Maintain a program of continued self-assessment for internal systems.
- Establish a strong relationship with the vendors serving House offices to ensure that security is an integral component of their system support and integration efforts.
- Ensure HOUSECIRT personnel excellence by continued exposure to the latest security information and technologies, self study, and active participation in professional organizations.

Other responsibilities include:

- Processing and responding to all House users' incident reports from intruder and malicious logic (virus) incidents.
- Evaluating, processing and assisting in deployment of countermeasures for all reported vulnerabilities.
- Establishing and maintaining information threat awareness to the House community.
- Assisting House Information Resources with computer attack damage control and recovery procedures. ”

HOUSECIRT

<http://www.house.gov/ushcert/mission.htm>



Appendix J

CSIRT Description for CERT Polska

<http://www.cert.pl/txt/rfc2350.txt>



-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

CSIRT Description for CERT Polska
=====

1. About this document

1.1 Date of Last Update

This is version 1.02, published on 7 March 2002.

1.2 Distribution List for Notifications

Currently CERT Polska does not use any distribution lists to notify about changes in this document.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the CERT Polska WWW site; its URL is <http://www.cert.pl/txt/rfc2350.txt>
Please make sure you are using the latest version.

1.4 Authenticating this document

This document has been signed with the CERT Polska PGP key. The signatures are also on our Web site, under:
<http://www.cert.pl/index3.html?id=12>
<http://www.cert.pl/english.html>

2. Contact Information

2.1 Name of the Team

"CERT Polska": Computer Emergency Response Team Polska

2.2 Address

CERT Polska
NASK
ul. Wawozowa 18
02-796 Warszawa
Poland

2.3 Time Zone

Central European Time (GMT+0100, GMT+0200 from April to October)

2.4 Telephone Number

+48 22 8208 274

2.5 Facsimile Number

+48 22 8208 399 (note: this is **not** a secure fax)

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

<cert@cert.pl> This is a mail alias that serves the human(s) on duty for CERT Polska.

2.8 Public keys and Other Encryption Information

CERT Polska has a PGP key, which KeyID is 0x553FEB09 and

which fingerprint is

D273 912B 6E00 49BA 3428 D485 07D7 5253

The key and its signatures can be found at the usual large public key servers.

2.9 Team Members

Mirosław Maj is the CERT Polska coordinator.

Other members of the team are:

Sławomir Gorniak

Przemysław Jaroszewski

Piotr Kijewski

Bartosz Kwitkowski

Ireneusz Parafjanczuk

Dariusz Sobolewski

Rafał Tarłowski

2.10 Other Information

General information about CERT Polska, as well as links to various recommended security resources, can be found at

<http://www.cert.pl/>

2.11 Points of Customer Contact

The preferred method for contacting CERT Polska is via e-mail at <cert@cert.pl>; e-mail sent to this address will be handled by the responsible human. We encourage our customers to use PGP encryption when sending any sensitive information to CERT Polska.

If it is not possible (or not advisable for security reasons) to use e-mail, CERT Polska can be reached by telephone during regular office hours. Off these hours incoming phone calls are transmitted to an answering machine. All messages recorded are checked ASAP.

CERT Polska hours of operation are generally restricted to regular business hours (08:00 - 17:00 CET Monday to Friday except holidays).

If possible, when submitting your report, use the form mentioned in section 6.

3. Charter

3.1 Mission Statement

The purpose of CERT Polska is to assist Polish internet users in implementing proactive measures to reduce the risks of computer security incidents and to assist them in responding to such incidents when they occur. CERT Polska also handles incidents that originate in Polish networks and are reported by any Polish or foreign persons or institutions.

3.2 Constituency

CERT Polska constituency is all hosts in .pl domain as well as all addresses assigned to NASK and other Polish internet providers.

3.3 Sponsorship and/or Affiliation

CERT Polska is financially maintained by the Research and Academic Network in Poland (NASK) which it is formally a part of.

3.4 Authority

CERT Polska operates under the auspices of, and with authority delegated by, Research and Academic Network in Poland (NASK).

CERT Polska expects to work cooperatively with system administrators and customers of NASK. All members of CERT Polska are employees of NASK and thus have wide possibilities of interacting with NASK System Administrators.

CERT Polska does its best to closely cooperate with all large ISP's abuse teams, establish direct contacts and exchange necessary data in order to prevent and recover from security incidents that affect their networks.

4. Policies

4.1 Types of Incidents and Level of Support

CERT Polska is authorized to address all types of computer security incidents which occur, or threaten to occur, in Polish networks.

The level of support given by CERT Polska will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the CERT Polska's resources at the time, though in all cases some response will be made within two working days.

Incidents will be prioritized according to their apparent severity and extent.

End users are expected to contact their systems administrator, network administrator, or department head for assistance. CERT Polska will give full support to the letter people. Only limited support can be given to end users.

4.2 Co-operation, Interaction and Disclosure of Information

CERT Polska exchanges all necessary information with other CSIRTs as well as with affected parties' administrators. No personal nor overhead data are exchanged unless explicitly authorized.

All sensible data (such as personal data, system configurations, known vulnerabilities with their locations) are encrypted if the must be transmitted over unsecured environment as stated below.

4.3 Communication and Authentication

In view of the types of information that CERT Polska deals with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

Where it is necessary to establish trust, for example before relying on information given to CERT Polska, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable level of trust. Within NASK, and with known neighbor sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members,

the use of WHOIS and other Internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

5. Services

5.1 Incident Response

CERT Polska will assist system administrators in handling the technical and organizational aspects of the incidents. In particular, it will provide assistance or advice with respect to the following aspects of incidents management:

5.1.1 Incident Triage

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

5.1.2 Incident Coordination

- Determining the initial cause of the incident (vulnerability exploited)
- Facilitating contact with other sites which may be involved.
- Facilitating contact with appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs
- Composing announcements to users, if applicable

5.1.3 Incident Resolution

CERT Polska will give advice but no physical support whatsoever to customers from outside of NASK internal network with respect to the incident resolution.

- Removing the vulnerability.
- Securing the system from the effects of the incident.
- Collecting the evidence of the incident.

In addition, CERT Polska will collect statistics concerning incidents processed, and will notify the community as necessary to assist it in protecting against known attacks.

To make use of CERT Polska's services please refer to section 2.11 for points of contact. Please remember that amount of assistance will vary as described in section 4.1

5.2 Proactive Services

CERT Polska coordinates and maintains the following services to the extent possible depending in its resources:

- Information services such as: list of security contacts, repository of security-related patches for various operating systems
- Training and educational services

CERT Polska organizes annual Secure conference covering current important security issues which is open for all interested parties.

Detailed information about obtaining these services is available from CERT Polska website at: <http://www.cert.pl/>

6. Incident Reporting Forms

CERT Polska had created a local form designated for

reporting incidents to the team. We strongly encourage anyone reporting an incident to fill it out, although this is never required. The current version of the form is available from:

<http://www.cert.org/formularz.txt>

Note: This form is only available in Polish.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT Polska assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.2 (GNU/Linux)

iQEVAwUBQ800UDpSGvtVP+sJAQIxrQf+MNxMuieymbDyKMDrStq1oUq5c1G81zTI
JdzKYHYczUqlG225mn0WGLnfbubH3Tkb9QzLVzZeDLki9qtvuCwawbAi3Bqdadwt
wFCE8ro4UQwAuqyvErsnuMBB0axgVslR8ehWag6Pgr5cNMejBqUwgeV+3rN/HIOg
Nv9yzcXqMSZilo2qlnBPgruGnMMVL8PPdtllaAiQgk7alTVClIn/eUZsJw+/laqH
u5amk+rNF5BZOijVocEUXoFq88tFcQxDoTu8m7oBNloABvOvn2EFV0jNqjC3KVLi
4E3OcWyXZ+oXlUqH3XSdjWPXNj+yOHJtlvC97uPWS+yLdL/lonFyIA==
=8aPA

-----END PGP SIGNATURE-----



Appendix K

Organizational Models





Organizational Models

This material is approved for public release.
Distribution is limited by the Software Engineering Institute to attendees.



Software Engineering Institute | Carnegie Mellon

© 2001-2008 Carnegie Mellon University

Alternative CSIRT Models

- Security Team
- Internal Distributed Team
- Internal Centralized Team
- Combined Distributed and Centralized Team
- Coordinating CSIRT



Here are some sample organizational models.

Each type of CSIRT Model has its strengths, weaknesses, and benefits.

What other models exist?

The model you choose will be based on

- where your constituency is located
- where your team is located
- what services you provide
- what information needs to be shared
- what type of actions need to take place
- what type of interactions need to take place

Security Team

Description:

- There is no identified CSIRT, incident response is handled by system, network, and security administrators as part of their day-to-day work

Strengths:

- staff is usually familiar with local systems and business functions
- reaction time can be faster at site

Weaknesses:

- no consistent response strategies
- no sharing of information - similar problems are not prevented
- no high level, organizational analysis



Having the responsibility for incident response remain at the local level creates several consequences. It appears that there is no current mechanism to set and to monitor minimum incident handling capabilities or incident response effectiveness.

This localized strategy does not provide for the ability to collect security data across the organization, to analyze that data to identify current and future threats, and to then alert the organization and distribute preventative and remedial actions.

Internal Distributed Team

Description

- local teams with centralized team lead

Strengths:

- information sharing can occur to create comprehensive analysis across the organization
- on site reaction time can be faster time

Weaknesses:

- time commitments can be an issue
- difficult to create a team synergy
- difficult to enforce consistent response effort



In this model, existing staff provides a “virtual” distributed CSIRT. There is a manager or team lead that oversees and coordinates activities affecting the virtual team. Across the organization, individuals are identified as the appropriate points of contact for particular functional areas or divisions, based on their experience and expertise with various operating-system platforms, technologies, and applications. These staff may perform incident handling on a full-time or part-time basis.

This virtual organization can be used to help set policy, enforce standards, and implement organization-wide incident response activity. Such a model also provides a capability for information to flow across the organization including obtaining incident reports and sharing response strategies.

If the team is composed of individuals with only part-time CSIRT responsibility, finding individuals with the appropriate experience, skills, and training, who are willing and able to take on these tasks, may be problematic. Once found and trained, these individuals need to be allowed to invest the time and energy to keep their skills and abilities current. This raises the possibility that the appropriate commitment from the operating units may not be sustained.

Effective management and coordination of this virtual organization may become a problem. It will take a strong central leader to develop a team spirit and keep all sites operating according to general standards.

Internal Centralized CSIRT

Description:

- CSIRT is centrally located, all team members spend 100% of their time on incident handling

Strengths:

- stable cadre of incident handling experts

good model for small organization

Weaknesses:

- there can be a delay in performing response efforts at local sites - may involve travel time
- difficult to enforce and standardize policies at sites



This model is one in which a fully staffed, dedicated CSIRT is given the resources to provide the services outlined in its charter. All team members spend 100% of their time working for the CSIRT. There is a team leader who reports to high-level management directly. The team is centrally located.

This dedicated CSIRT model provides a very stable structure for building incident handling capabilities, and makes those capabilities manageable and predictable. It provides the organization with a clear mechanism for proactively managing its computer security risks. The organization can now analyze potential threats and risks and determine the appropriate levels of prevention and mitigation necessary to provide adequate levels of response.

This model requires that a new specialized unit be created, staffed, and integrated into the organization's operations.

The main weakness of this model is that now the incident handling capability is separate and distinct from the operational units. In a small organization this should not be a problem.

In a large organization it may be difficult for the CSIRT to keep up to date with changing technologies across geographically dispersed sites. It may also become difficult for the dedicated team to integrate and coordinate across a large organization. There is also no mechanism to ensure that response efforts are being carried out in a consistent, correct manner at the local level.

Combined Distributed and Centralized Team

Description:

- a centralized team with distributed members across geographic or functional sites

Strengths

- best of centralized and distributed models
- mechanism for information sharing, analysis, and standardized responses

Weaknesses:

- two structures to maintain
- still difficult to ensure conformance



This model is an attempt to combine the best features of the virtual model with the best features of the centralized model. It maximizes the utilization of existing staff in strategic locations throughout the organization with the centrally located coordinating capabilities of the dedicated team to provide a broader understanding of the security threats and activity affecting the constituency.

The strengths of this model are that it provides a stable core of full-time CSIRT professionals along with a network of part-time affiliated members in the operating units. The full-time members provide the stability, expertise, and permanent infrastructure, while the part-time members provide the operational knowledge and ability to involve the operational units. This provides a better possibility for acceptance or “buy-in” from all parts of the organization.

The greatest weakness of this approach is that now there are two systems that must be managed and coordinated. If this is not handled well the result will be a disconnected dedicated team along with an ineffectual distributed component.

Coordinating CSIRT

Coordinating CSIRTs facilitate incident handling and analysis across numerous CSIRTs or organizational units.

They facilitate information sharing and dissemination relating to

- incident trends, patterns, and activity
- response and mitigation strategies
- analysis and research
- new tools and techniques for incident handlers



A CSIRT can also be organized as a coordinating center rather than a one-on-one incident response service. In this case, the CSIRT helps organize response efforts across dispersed, geographic teams or even across business units throughout an organization. These dispersed groups carry out the actual incident response steps and mitigation strategies. The coordinating CSIRT synthesizes incident reports and statistics from all areas to determine the general security position of the organization and its vulnerability to attack. It also is able to consolidate the information so that an accurate picture of incident activity across the organization can be relayed as needed.

As a coordinating center, a CSIRT might also act as a major reporting center for a number of constituencies or other CSIRTs. They may also coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broad community.

CSIRTs being set up for a country or a state or province would most likely be a coordinating CSIRT.

The CERT/CC in its role as a coordination center facilitated collaboration between various CSIRTs during the Y2K effort. They have also brought together experts in the field for workshops on Distributed Denial of Service tools and activities and on security in ActiveX.

The results of these workshops can be found at:

Results of the Distributed-Systems Intruder Tools Workshop:

http://www.cert.org/reports/dsit_workshop-final.html

Results of the Security in ActiveX Workshop

http://www.cert.org/reports/activeX_report.pdf



Appendix L

Creating and Managing a CSIRT Action Plan



Action Plan:

Instructions:

The Action Plan has two parts. Part 1 is for you to identify any actions you want to take once you return to your organization. Part 2 contains a checklist of various issues you can use to benchmark your planning activities if you are building a CSIRT and your operational activities for an existing CSIRT.

You do not have to be performing all activities, but this plan can help you prioritize where you want to focus any improvement activities.

Part 1:

This document can be used to help organize your thoughts and your proposed actions that result from the workshop discussions. These might include:

- organizing your answers to questions we ask during the course that are specific to your organization
- identifying people that you need to involve in the CSIRT development process
- identifying issues that need to be addressed at your site and also identifying to whom they should be addressed
- highlighting ideas you have for how your CSIRT should operate or specific improvements you want to make

Part 2:

Use your Action Plan to benchmark your team against the various planning and operational practices. Note all the major issues and practices that you have already addressed by placing an "x" or a checkmark in the designated box.

Once you are back at your site, you can use this Action Plan as a reminder of issues that need to be addressed. It can also be used to highlight questions you want to discuss with your sponsors, management, CSIRT staff, or other related stakeholders.

Revisit this Action Plan periodically; see what other items you have completed and can check off. Do this on a weekly, monthly, and yearly basis, as appropriate.

Action Plan:

Part 1: Actions to Take:

- **What two best practices do you want to implement for your team?**

- **What two process improvements do you want to make?**

- **Are there any other internal or external entities for which you need to establish a formal interface or communications channel?**

- **What are your highest priorities?**

Part 2: Benchmarking Practices:

Creating an Effective CSIRT

Planning Your CSIRT – if you are still in the planning stages

- Do you know who your stakeholders are?
- Do you have a CSIRT or Incident Management Capability (IMC) Development Project Team?
- Have you established a methodology for the Project Team?
- Have you established communication mechanisms for gathering and sharing data in the Project Team and throughout the organization?
- Has your Project Team read available resources about incident management or CSIRTs such as the Handbook for CSIRTs?
- Do you have a list of the information you need to gather?
- Do you know who you need to talk to at your organization to get the information you need?
- Have you included the system and network administrators?
- Have you included any existing security groups or personnel?
- Have you included human resources?
- Have you included the legal department?
- Have you included the public relations department?
- Have you included anyone from audits or risk management?
- Have you included all department and division or constituency managers?
- Have you included representatives from your end-user constituency?
- Have you included other relevant parties such as: _____

- Have you highlighted and addressed any business or organizational issues and constraints that may affect the creation of your CSIRT or IMC?
- Have you collected information on existing response statistics that can be used for comparison after the capability is operational to gauge its effectiveness?
- Have you identified what processes related to incident management are already occurring in your organization or constituency?
- If appropriate, have you outline the process workflows for your “as-is” state; that is how you are currently performing incident management functions?
- Have you identified how a CSIRT or IMC will fit into the existing processes?
- Have you identified what processes may need to be changed?

- Have you determined what part of the incident management processes your CSIRT will have responsibility for?
- Have you established a vision for your CSIRT or IMC?
- Have you documented this vision in a Concept of Operations document?
- Have you discussed this vision with the rest of the organization?
- Do you have management support for your vision? (Have you met with management and presented the vision to them and received approval and defined resources, budget, and timeframe?)
- Do you have organizational support for your vision? (Have you met with functional business managers and representatives from your end-user community to present the vision to them and get their buy-in?)
- Do you have funding for your CSIRT or IMC establishment?
- Have you developed a long-term funding plan?
- Has the CSIRT or IMC plan been announced by management to the organization and constituency?
- Have you created an implementation plan?
- Has the plan been announced and released to the rest of the organization or constituency?
- Have you received feedback on the plan and updated it accordingly?
- Have you talked to all areas of the organization or constituency so they understand any change in procedures or process when the CSIRT or IMC becomes operational?

Have you identified your CSIRT Components?

- Do you have a defined constituency? Who is it? _____
- Do you have an identified mission?
- Have you developed a mission statement to explain your mission?
- What is your basic mission: _____

- In the development of your mission, if you are building a CSIRT, have you answered the following questions:
- Will the CSIRT perform any recovery and repair of systems?
 - Will the CSIRT perform any computer forensics tasks?
 - Will the CSIRT perform any network monitoring or IDS/IPS monitoring?
 - Will the CSIRT provide maintenance of external defenses such as the firewall?
 - Will you work in any way with law enforcement?

- If yes, have you determined when and how you will contact law enforcement?
- Have you selected the services your CSIRT or IMC will provide?
- Have you defined the roles and responsibilities for each service?
- Have you defined these services for internal and external audiences?
- Have you established your CSIRT or incident management policies?
 - CSIRT charter that explains the purpose, operating hours, and services of the CSIRT?
 - Acceptable use policy that outlines the appropriate use of CSIRT or IMC equipment, systems, and software by CSIRT or IMC staff?
 - Information Dissemination policy that explains what information can and cannot be released and who is authorized to receive such information?
 - Media relations policy that defines who handles all media questions and what that corresponding process is?
 - Engagement of law enforcement policy that explains when and how law enforcement is contacted?
 - Incident Reporting Policy that describes to the constituency where and how incidents are to be reported?
 - Publication Policies that defines the types of publications your team will publish and the process for doing that?
- Have you developed corresponding procedures for your policies and services?
- Have you chosen an organizational model for your CSIRT or IMC?
- If your model is an “ad hoc” model, have you determined what will triage its engagement?
- If your model is an “ad hoc” model, have you determined who will triage its engagement?
- Do you know where the CSIRT or IMC fits in your organization chart?
- Do you know to whom the CSIRT or IMC will report?
- Have you determined the authority of the CSIRT or IMC?
- Do you have management support for this authority?
- Has management told the rest of the organization about this authority information?
- If appropriate, have you developed process workflows for your “to be” state, that is the process changes that will be implemented when your CSIRT or IMC becomes operational?
- If you have documented a “to be” state, have you shared this information with the rest of the organization or constituency and obtained consensus, approval, and support for the changes?

- Have you determined all roles and responsibilities related to your CSIRT or IMC?
- Have you identified the staff positions to fulfill those roles?
- Have you developed job descriptions for each position, where necessary?
- Have you identified a team lead for the CSIRT or IMC?
- Do you know where you will get this staff from: existing internal, hiring new external, contracting, etc.?
- If you will be sending out alerts or developing technical documents, have you made arrangements to get the assistance of technical writers?
- Do you have a physical location for the CSIRT or IMC staff?
- Does this location have secured access to protect the staff?
- Have you identified the equipment your CSIRT or IMC staff requires?
- Have you identified the specific infrastructure requirements your CSIRT or IMC staff will need?

Incident Management Processes and Operational Practices

If your CSIRT or IMC is already established

- Have you published your CSIRT or IMC contact information: phone, email, web site?
- Do you have an up-to-date organization chart for your CSIRT or IMC.
- Does your organization have a consistent definition and criteria for what constitutes an “incident”?
- Has this criteria been institutionalized (taught throughout the organization)?
- Have you established standardized categorization and prioritization criteria for incidents?
- Is there agreement on who will need to be involved and notified during an incident?
- Does your organization or constituency have a site security policy?
- If you have a site security policy, is it consistent with the criteria for what constitutes an incident?
- Have you published a document that describes your services for your constituency?
- Have you established information and incident reporting guidelines?
- Have you released an incident reporting form (if appropriate)?
- Do you have an established process for reporting PII incidents (incidents where Personally Identifiable Information was released in an unauthorized fashion)?
- Is there an escalation process in place if assistance is needed from management?
- Do you record and track incidents in an incident tracking system?

- Does your incident tracking system perform incident correlation?
- Do you have an established data retention policy and procedure in place for archived incident data and supporting materials like logs and emails?
- Do you have a communications plan – a list of people to be notified as part of your incident response plan?
- Is this list in both hardcopy and electronic format?
- Have you released information about any public keys that your constituency should use?
- Do you have a published incident response plan that explains the basic response activities to your constituents?
- Have you documented an incident response plan for each category of incident you have defined that describes what actions must be taken and who must be involved and notified?
- Do you know with whom your CSIRT or IMC will need to collaborate or coordinate with?
- Have you established defined interfaces, Points of Contact, communication channels, and other internal or external areas that you will collaborate or coordinate?
 - Group responsible for patch management
 - Group responsible for vulnerability scanning and management
 - Group responsible for network monitoring
 - Group responsible for anti-virus scanning and updates
 - Group responsible for external defenses: IDS, Firewalls, routers, etc.
 - Legal counsel
 - Human resources
 - Media relations
 - Risk management
 - ISPs
 - Law enforcement
- Do you have appropriate non-disclosure agreements in place with all external collaborators?
- Is the CSIRT represented on any configuration or change management committees?
- Is the CSIRT represented on any security boards or councils within the organization?
- Do you have a CSIRT or IMC public web site?
- Do you have defined document types and publication instructions?
- Have you chosen a method for secure communications with your constituency (such as PGP, S/MIME, Digital Certificates)?

- If staff will have home equipment, is there a means for secured remote access from this equipment to the CSIRT or IMC systems?
- Have you established a backup site in case of disaster?
- Have you tested moving your staff and services to the back up site?
- Do staff know and understand your CSIRT or IMC Acceptable Use Policy?
- Do you have a mentoring and training program in place for staff?
- Is there a professional development program in place for staff?
- Do you have an operational security program in place for CSIRT or IMC staff?
- Have CSIRT and IMC staff been trained how to handle PII information?
- Are there regular operational or mock exercises done as team building and training exercises for the CSIRT or IMC.
- Have you provided security awareness training to the constituency?
- Have you identified what information will come into your CSIRT or IMC?
- Have you determined how the information will flow out of your CSIRT or IMC?
- Are you receiving information from
 - Vulnerability scanning
 - Risk analysis
 - Network monitoring
 - Situational awareness (political, economic, social events and news, but security news)
 - Public monitoring or technology watch
 - Vendor and vulnerability disclosure sites
- Are you providing input into
 - Configuration management decisions for constituent systems
 - Software and hardware purchases and deployment based on security issues
 - Security awareness training for end-users
 - Patch management decisions and deployment
 - Defense-in-depth strategies for constituent networks
- If appropriate, have you worked with risk management to get the results of any risk analyses that have been done to determine what threats and resulting impacts exist for the organization's critical assets.
- Have you used the results of the risk analysis to help build any incident response plans?
- Have you worked with the rest of the organization to determine what critical assets must be protected and their priority?

- Is there an organizational information classification scheme in place that identifies and distinguishes between public, sensitive or confidential information?
- Do your incident reporting, response, and escalation policies and procedures include instructions for handling each type of information?
- Do you do any trend analysis on submitted incidents and vulnerabilities from your constituency?
- Do you have defense-in-depth strategies in place to protect CSIRT or IMC systems and networks?
- Have you established a formal method for evaluating that your CSIRT or IMC is meeting its mission and constituent needs?