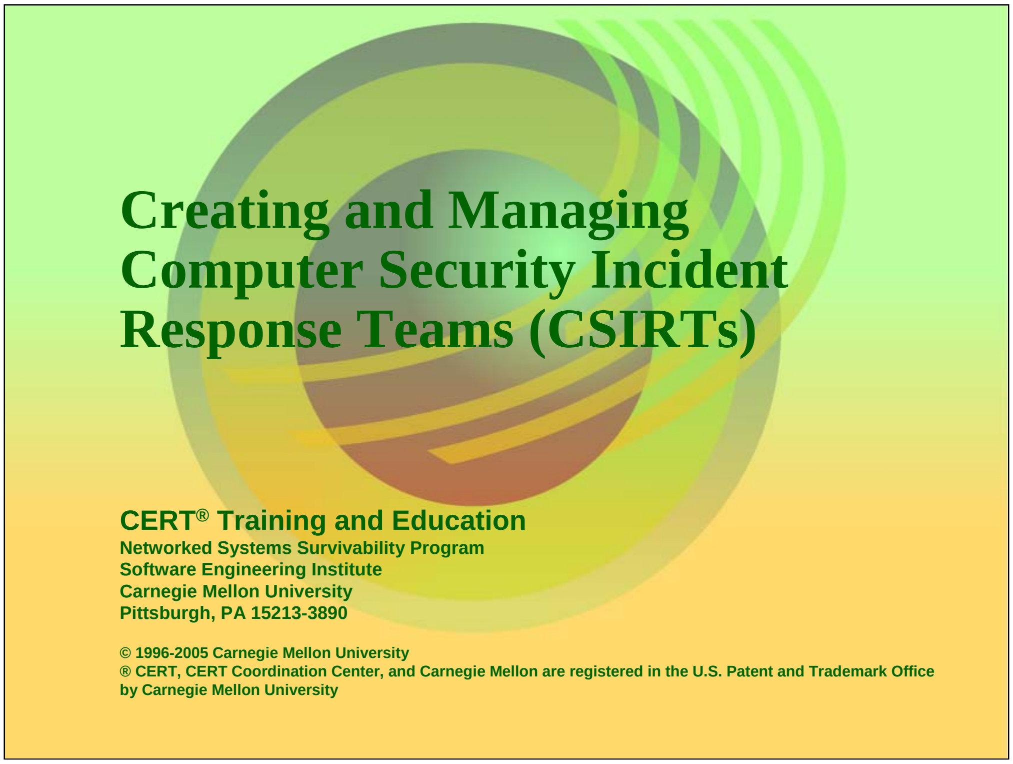


# Creating and Managing Computer Security Incident Response Teams (CSIRTs)

**CERT® Training and Education**
Networked Systems Survivability Program
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

The CERT® Coordination Center (CERT/CC) is located at 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.

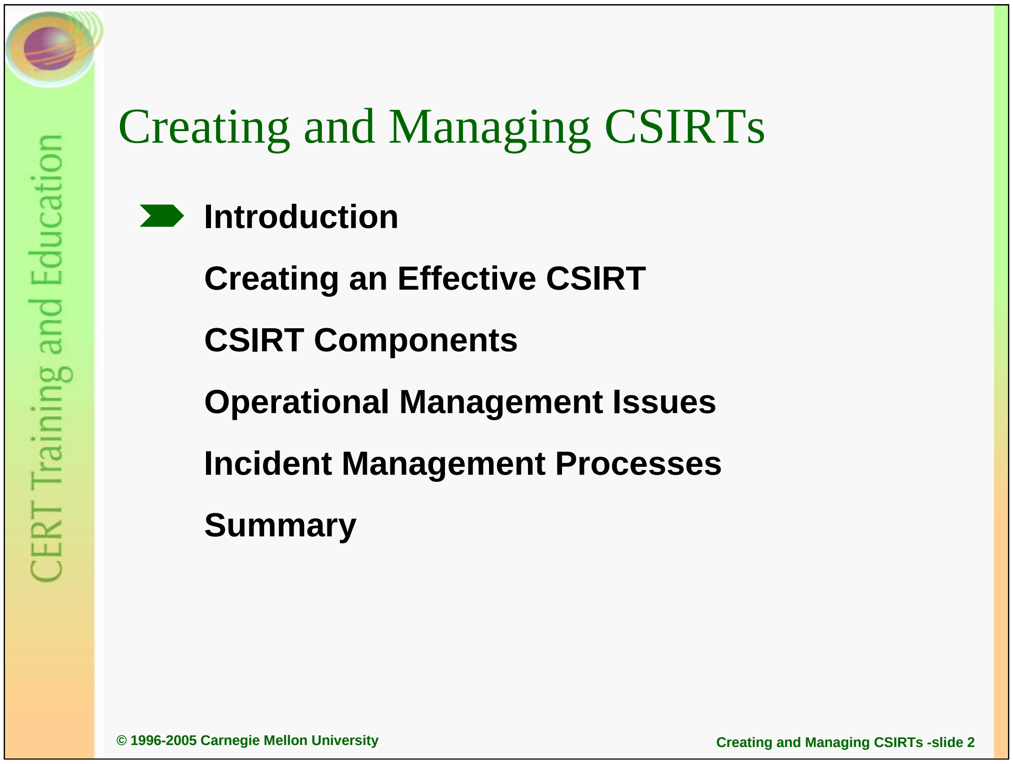
While we continue to respond to security incidents and analyze product vulnerabilities, our role has expanded over the years. Along with the rapid increase in the size of the Internet and its use for critical functions, there have been progressive changes in intruder techniques, increased amounts of damage, increased difficulty of detecting an attack, and increased difficulty of catching the attackers. To better manage these changes, and align our areas of work and research, the CERT/CC is now part of the larger SEI Networked Systems Survivability (NSS) Program.

The primary goal of the NSS Program is 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.

The CERT/CC charter is to work with the Internet community in detecting and resolving computer security incidents as well as taking steps to prevent future incidents. Our specific mission is to

- provide a comprehensive view of attack methods, vulnerabilities, and the impact of attacks on information systems and networks; provide information on incident and vulnerability trends and characteristics
- build an infrastructure of increasingly competent security professionals who respond quickly to attacks on Internet-connected systems and are able to protect their systems against security compromises
- provide methods to evaluate, improve, and maintain the security and survivability of networked systems
- work with vendors to improve the security of as-shipped products

Parts of this work were derived from work originally sponsored by the U.S. Army Land Information Warfare Activity (LIWA) and the U.S. Defense Information Systems Agency (DISA).



CERT Training and Education

## Creating and Managing CSIRTs

- Introduction
- Creating an Effective CSIRT
- CSIRT Components
- Operational Management Issues
- Incident Management Processes
- Summary

Creating and Managing CSIRTs -slide 2

Introduction

Creating an Effective CSIRT

- What is a CSIRT?
- What Does a CSIRT do?
- General Categories of CSIRTs
- Building Your Vision
- Implementation Recommendations

CSIRT Components

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

Operational Management Issues

- CSIRT Staffing Issues
- Managing CSIRT Infrastructures
- Evaluating the CSIRT’s Effectiveness

Incident Management Processes

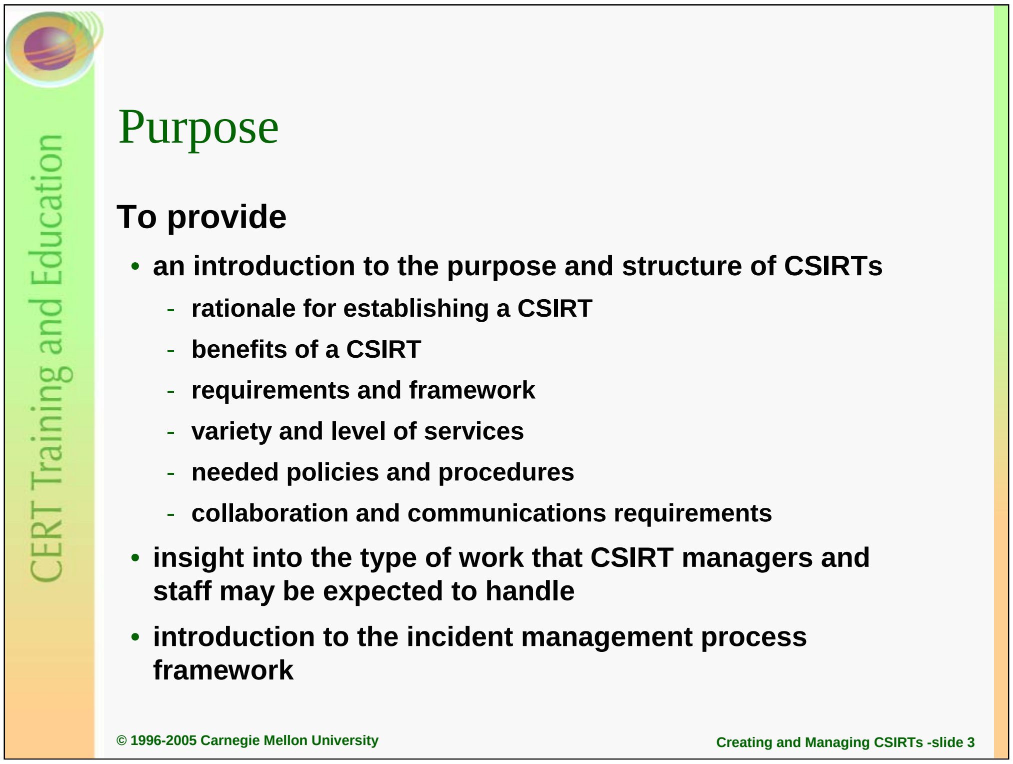
- Critical Information
- Prepare/Improve/Sustain
- Protect Infrastructure
- Detect Events
- Triage Events
- Respond

Summary

---

Presenters:
Audrey Dorofee
David Mundie
Robin Ruefle

CERT CSIRT Development Team
CERT Training and Education
Networked Systems Survivability
Software Engineering Institute
Carnegie Mellon University
http://www.cert.org/csirts/



CERT Training and Education

## Purpose

**To provide**

- **an introduction to the purpose and structure of CSIRTs**
  - **rationale for establishing a CSIRT**
  - **benefits of a CSIRT**
  - **requirements and framework**
  - **variety and level of services**
  - **needed policies and procedures**
  - **collaboration and communications requirements**
- **insight into the type of work that CSIRT managers and staff may be expected to handle**
- **introduction to the incident management process framework**

Creating and Managing CSIRTs -slide 3

This tutorial presents a high level overview of the management, organizational, and procedural issues involved with creating and operating a Computer Security Incident Response Team (CSIRT).

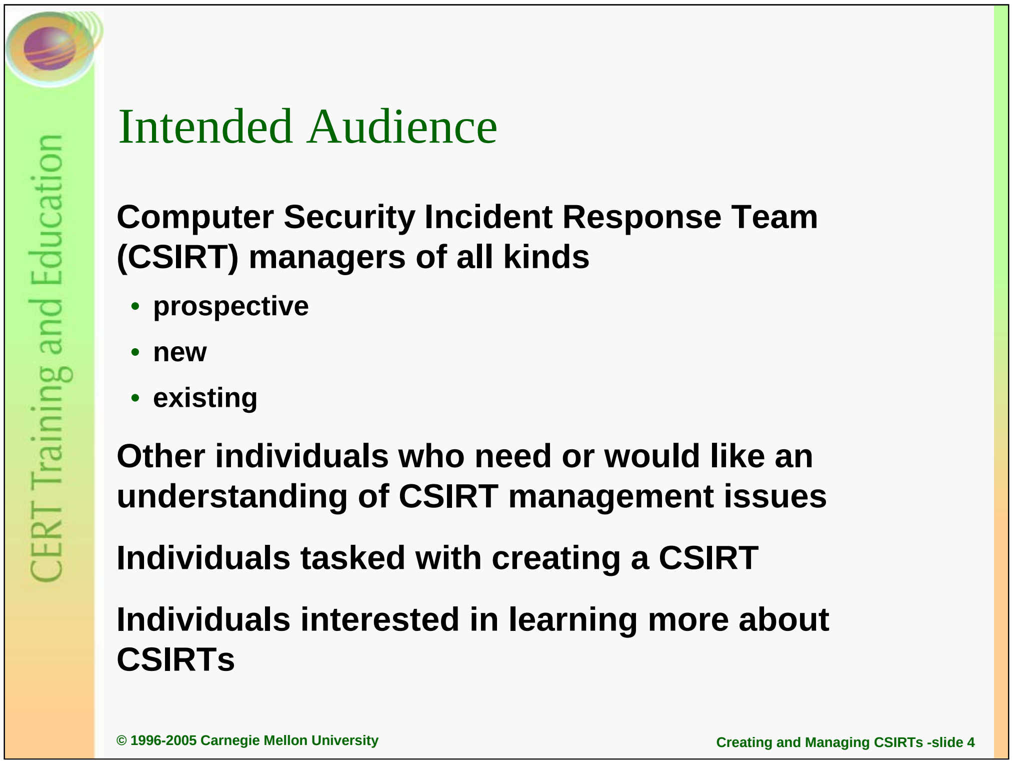
This session will provide an introduction to the purpose and structure of CSIRTs. This will include the

- rationale for establishing a CSIRT
- benefits of a CSIRT
- requirements and framework for establishing an effective CSIRT
- variety and level of services that can be provided by a CSIRT
- policies and procedures that should be established and implemented for a CSIRT
- importance of collaboration and communications within and across teams

The session will provide insight 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

- identifying critical information
- providing the hotline and triage functions
- coordinating response
- managing the CSIRT infrastructure
- protecting CSIRT data
- hiring CSIRT staff

This tutorial will also present a best practice model for performing incident management.



CERT Training and Education

## Intended Audience

**Computer Security Incident Response Team (CSIRT) managers of all kinds**

- **prospective**
- **new**
- **existing**

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

**Individuals tasked with creating a CSIRT**

**Individuals interested in learning more about CSIRTs**

Creating and Managing CSIRTs -slide 4

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.

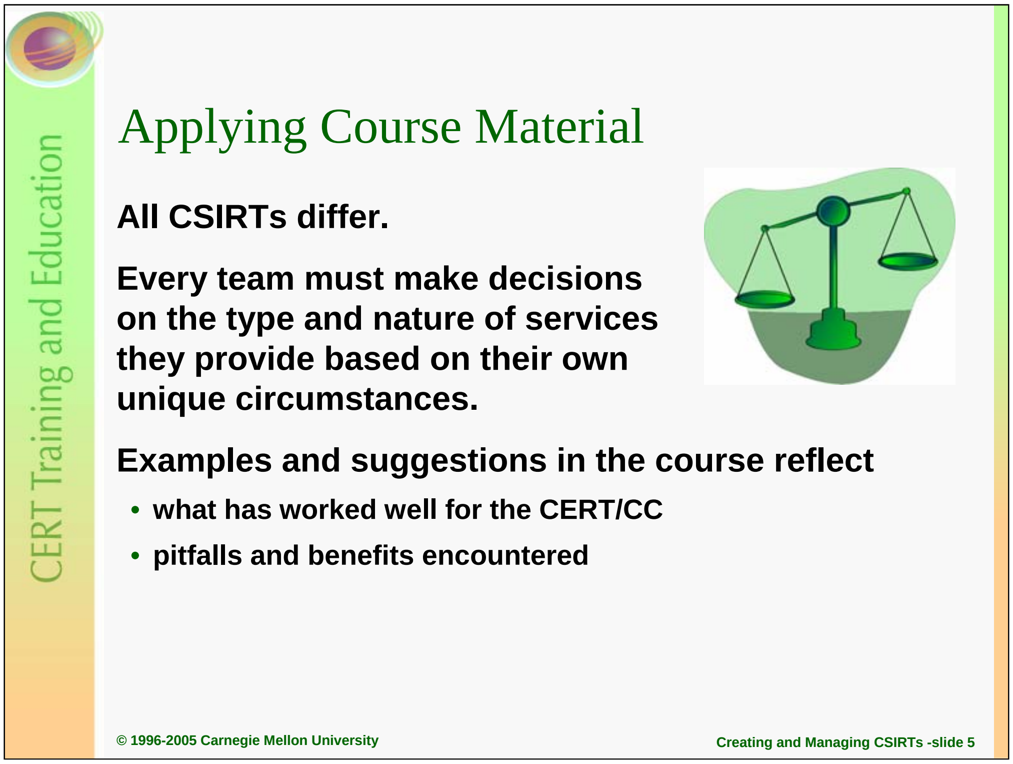
Individuals tasked with creating a CSIRT might include

- chief information officers (CIOs)
- chief security officers (CSOs)
- managers
- project leaders
- project team members
- other interested or relevant parties

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
- upper management
- risk management and audit staff
- constituency members

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



CERT Training and Education

# Applying Course Material

**All CSIRTs differ.**

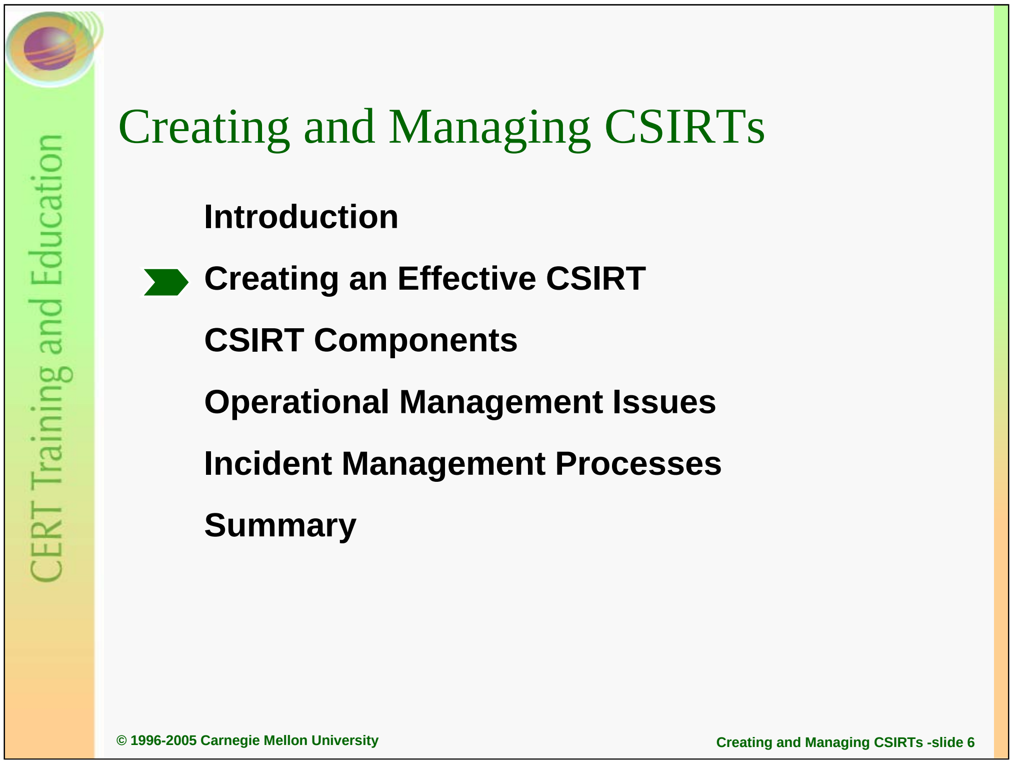
**Every team must make decisions on the type and nature of services they provide based on their own unique circumstances.**

**Examples and suggestions in the course reflect**

- **what has worked well for the CERT/CC**
- **pitfalls and benefits encountered**

Creating and Managing CSIRTs -slide 5

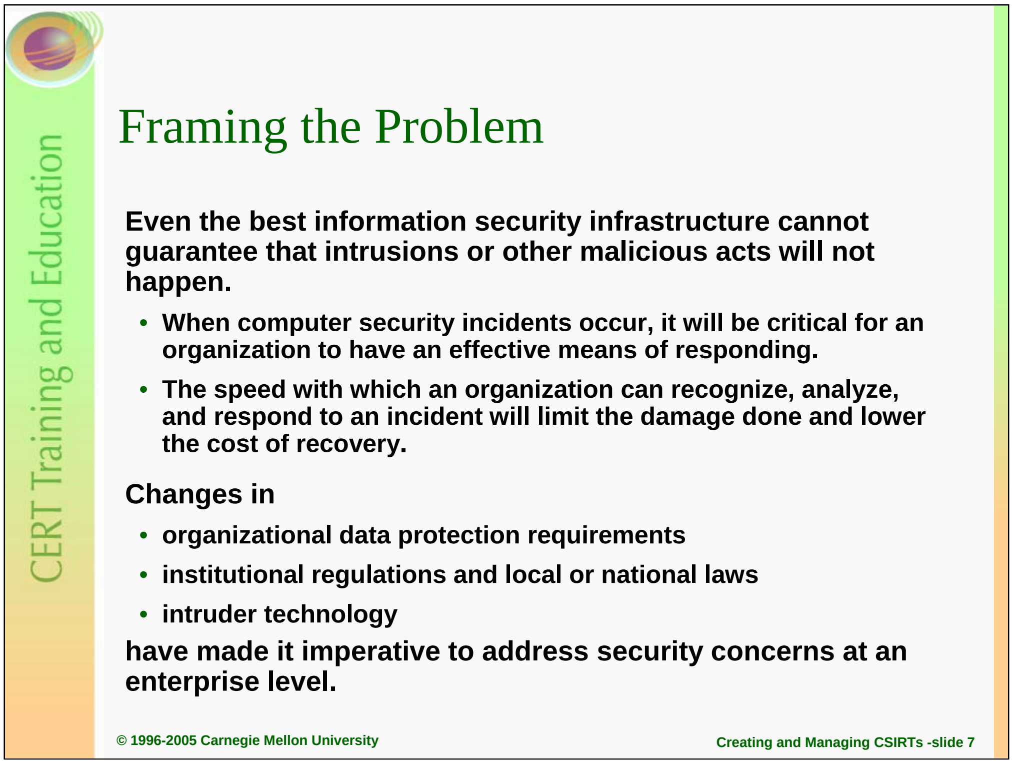
Note that not all CSIRT teams are alike. We cannot give definitive answers about the best way to address a particular issue for your CSIRT. Apply your team’s criteria to each situation. Take this information and apply what works for your organization.



CERT Training and Education

## Creating and Managing CSIRTs

- Introduction
- ➤ Creating an Effective CSIRT
- CSIRT Components
- Operational Management Issues
- Incident Management Processes
- Summary



CERT Training and Education

## Framing the Problem

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

- **When computer security incidents occur, it will be critical for an organization to have an effective means of responding.**
- **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.**

**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.**

Creating and Managing CSIRTs -slide 7

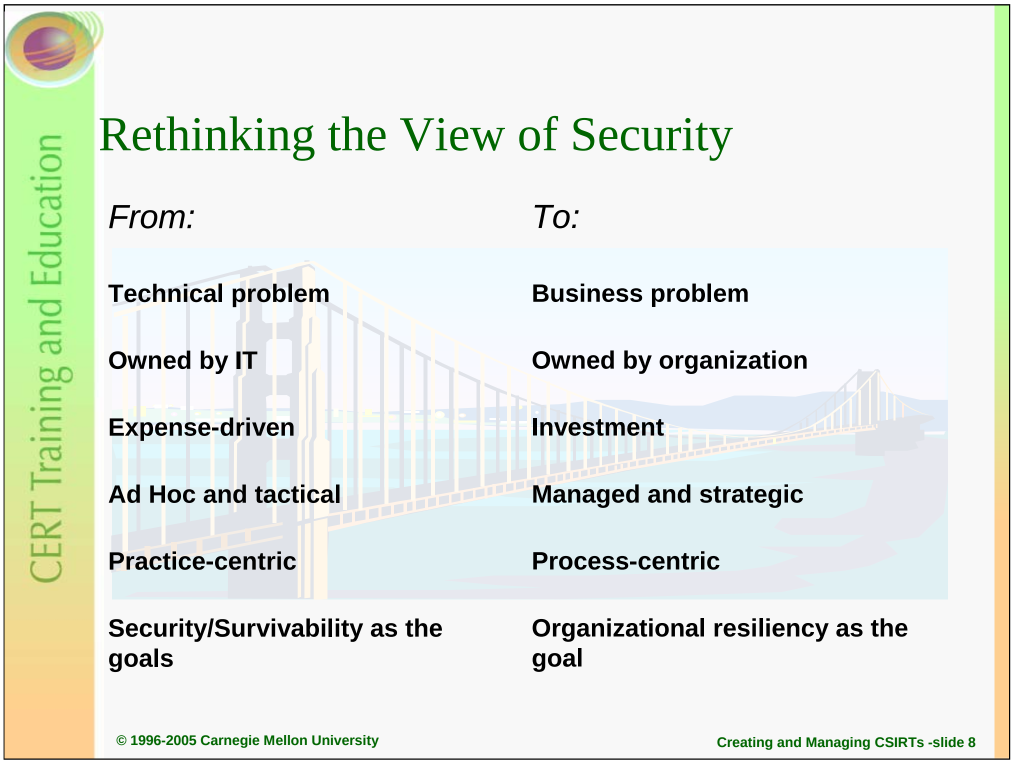
The Internet has become an infrastructure itself and as such must be protected to ensure reliable, stable service. Network and system administrators do not have the people and practices in place to defend against attacks and minimize damage, on their own.

New rules and regulations are being introduced to ensure data protection and accountability. This can have an impact on the security policies and procedures required for an organization. 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.
- California Security Breach Information Act (SB-1386) – "is a California state law requiring organizations that maintain personal information about individuals to inform those individuals if the security of their information is compromised. The Act stipulates that if there's a security breach of a database containing personal data, the responsible organization must notify each individual for whom it maintained information." <http://searchcio.techtarget.com/sDefinition/0,,sid19_gci951441,00.html>

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

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



CERT Training and Education

## Rethinking the View of Security

| *From:* | *To:* |
|---|---|
| **Technical problem** | **Business problem** |
| **Owned by IT** | **Owned by organization** |
| **Expense-driven** | **Investment** |
| **Ad Hoc and tactical** | **Managed and strategic** |
| **Practice-centric** | **Process-centric** |
| **Security/Survivability as the goals** | **Organizational resiliency as the goal** |

Creating and Managing CSIRTs -slide 8

Part of other work being done at the Software Engineering Institute focuses on Enterprise Security Management (ESM). ESM looks at security from a different perspective. CSIRTs, and more broadly incident management, is a part of this Enterprise level, and many of the same shifts in thinking about security management are also applicable to incident management.

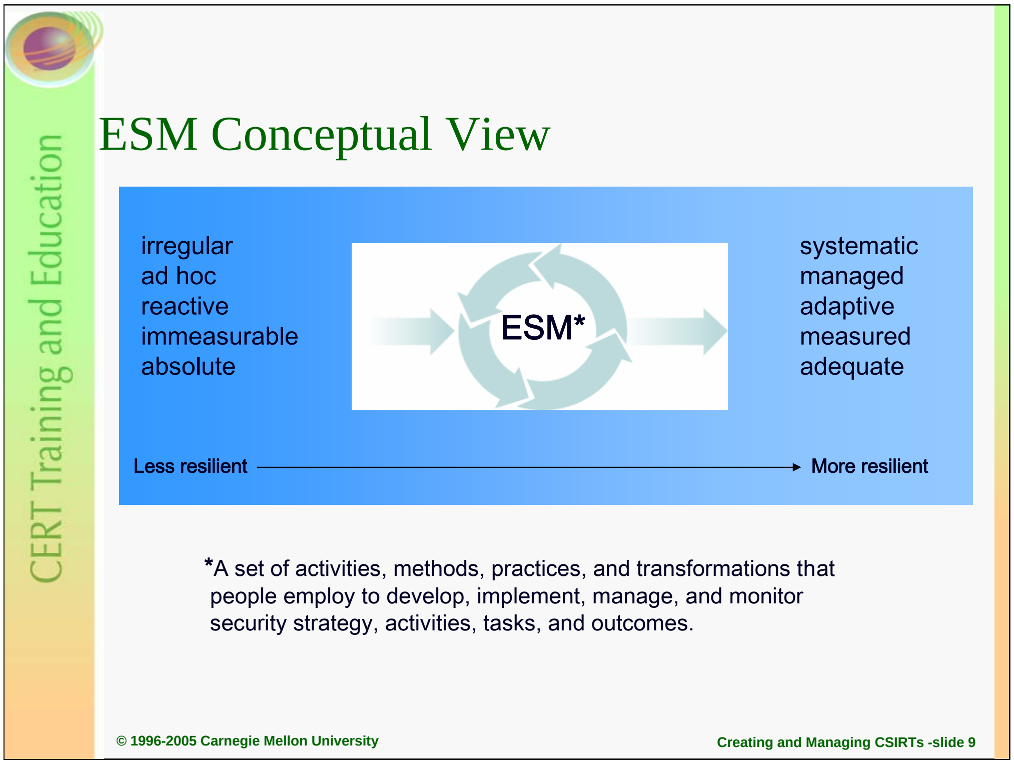
To deal with these challenges (to “get there from here”), and to address the inevitable new challenges that new  risks bring, organizations must evolve in their abilities and capabilities to manage security—moving from the current state noted on the left part of the above slide to the state described on the right.

This means 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.

For the CSO, it means that they must be 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.

The same holds true for incident management.



CERT Training and Education

# ESM Conceptual View

irregular
ad hoc
reactive
immeasurable
absolute

ESM*

systematic
managed
adaptive
measured
adequate

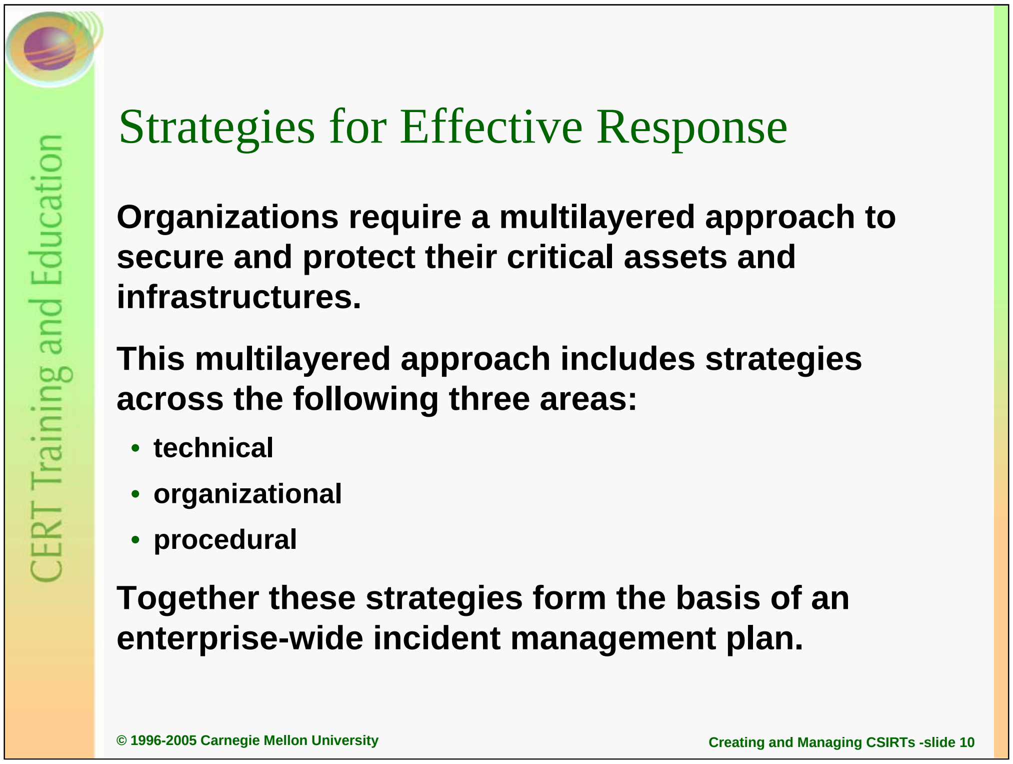
Less resilient → More resilient

*A set of activities, methods, practices, and transformations that people employ to develop, implement, manage, and monitor security strategy, activities, tasks, and outcomes.

Enterprise security management (ESM) is an emerging body of work in the NSS program that is focused on helping organizations to evolve and improve the effectiveness and outcomes of their security efforts.  In essence, ESM is about helping organizations do security in a way that enables its critical assets and processes and contributes to the organization’s resiliency.

ESM is a way for organizations to evolve their security approach from one that is ad hoc and reactive to one that is coordinated, systematic, adaptive, and measured.

ESM in the broad sense can be described as a set of activities, methods, practices, and transformations that people employ to develop, implement, manage, and monitor security strategy, activities, tasks, and outcomes.  In short, ESM is the process and tool kit that organizations need to evolve their security approach to a level of organizational resiliency that is required to achieve their goals and accomplish their mission.


CERT Training and Education

## Strategies for Effective Response

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

**This multilayered approach includes strategies across the following three areas:**

- **technical**
- **organizational**
- **procedural**

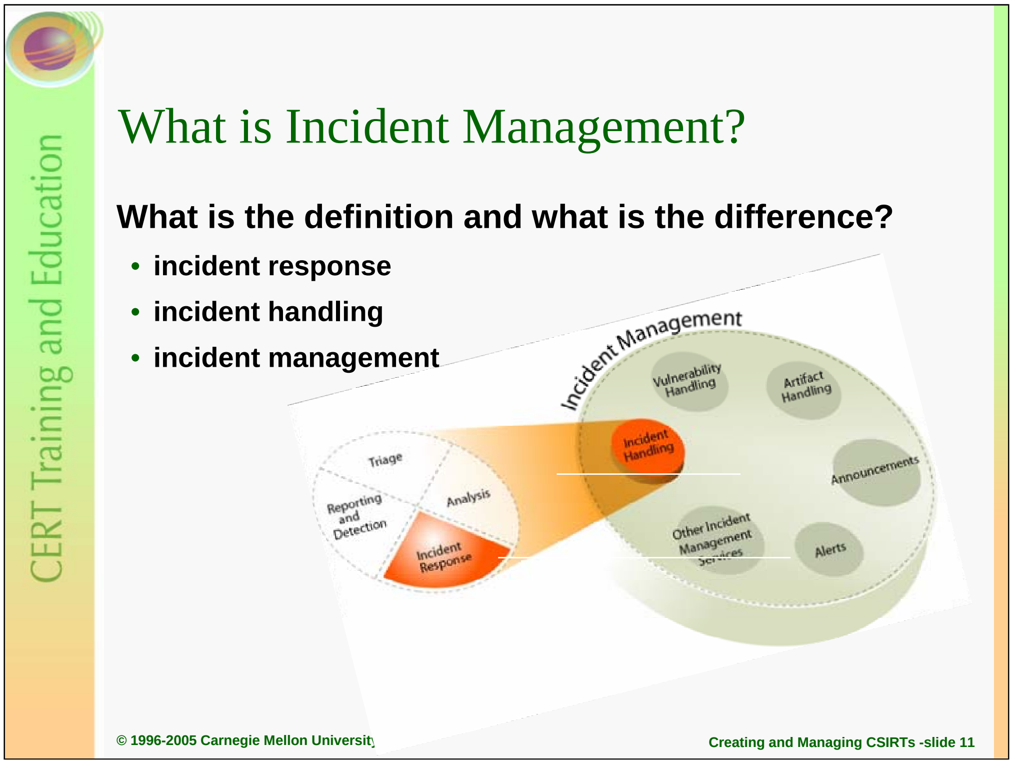
**Together these strategies form the basis of an enterprise-wide incident management plan.**

Creating and Managing CSIRTs -slide 10

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 computer security 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.

As a defense against Internet security threats, organizations can

- 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 computer security policies and procedures
- provide security awareness training to employees, customers, and constituents
- create an incident management capability



CERT Training and Education

## What is Incident Management?

**What is the definition and what is the difference?**

- **incident response**
- **incident handling**
- **incident management**

© 1996-2005 Carnegie Mellon University

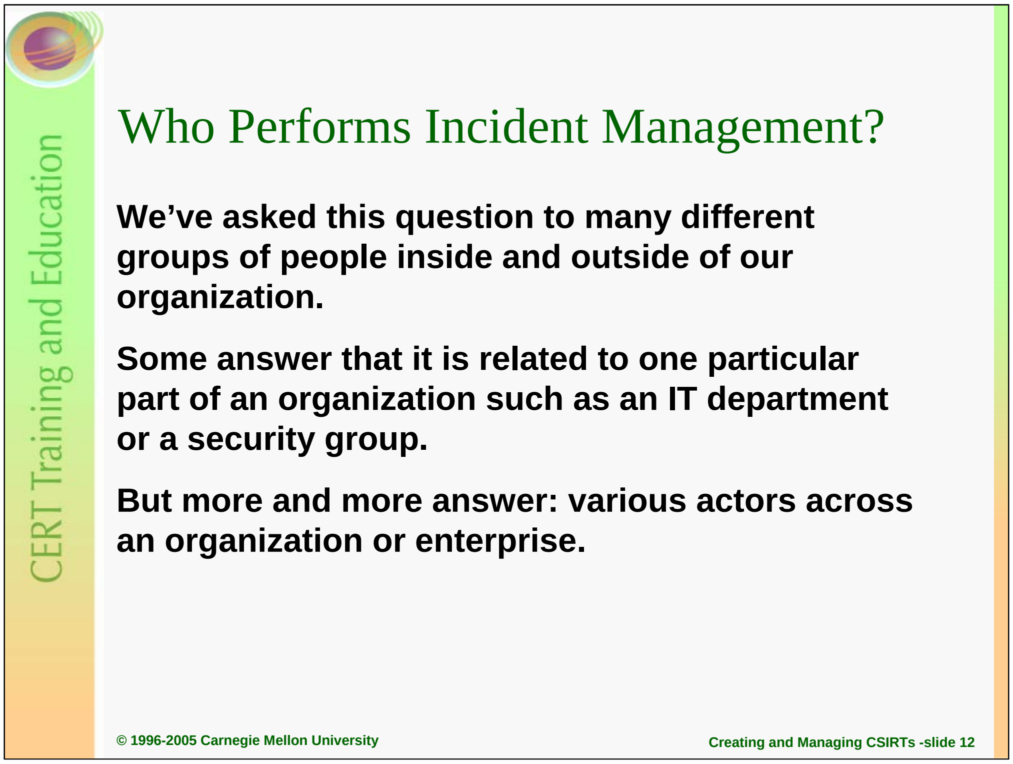
Creating and Managing CSIRTs -slide 11

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.

The term “incident management” expands the scope of this work to include the other services and functions that may be performed, including vulnerability handling, artifact handling, security awareness training, and other services. The definition of this term to include this expanded set of services is important because incident management is not just responding to an incident when it happens. It also includes proactive activities that help prevent incidents by providing guidance against potential risks and threats, for example, identifying vulnerabilities in software that can be addressed before they are exploited. These proactive actions include training of end users to understand the importance of computer security in their daily operations and to define what constitutes abnormal or malicious behavior, so that end users can identify and report this behavior when they see it. Some of these tasks may be done by persons outside of the normal security department or CSIRT function.



CERT Training and Education

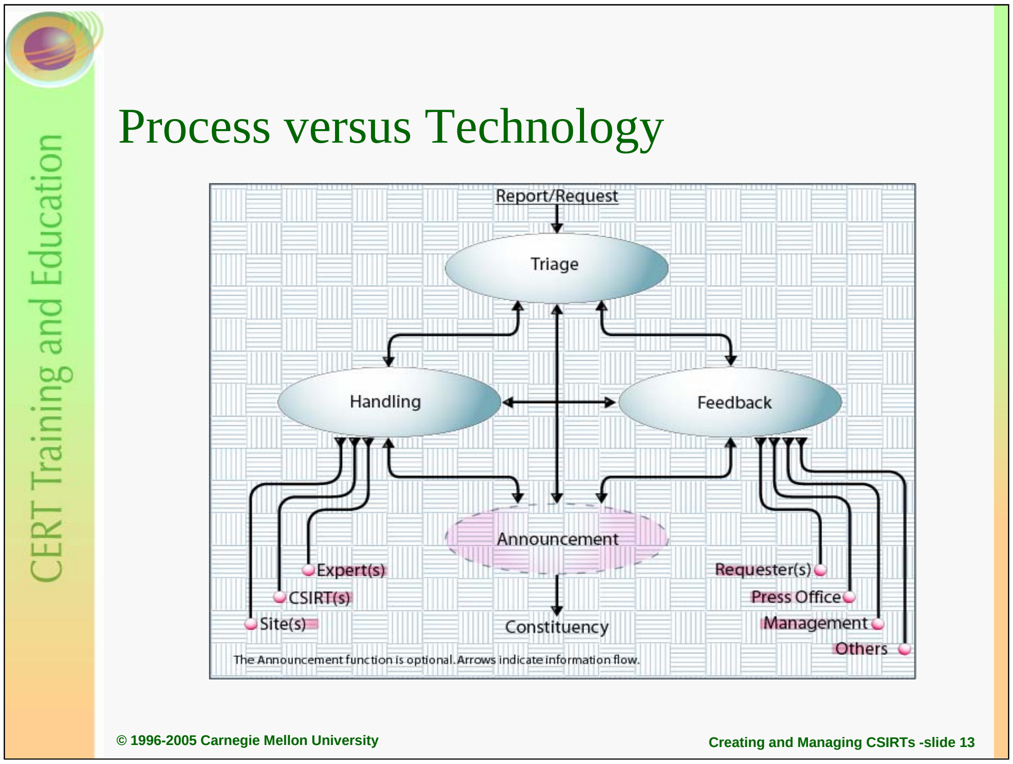
## Who Performs Incident Management?

**We’ve asked this question to many different groups of people inside and outside of our organization.**

**Some answer that it is related to one particular part of an organization such as an IT department or a security group.**

**But more and more answer: various actors across an organization or enterprise.**

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.



CERT Training and Education

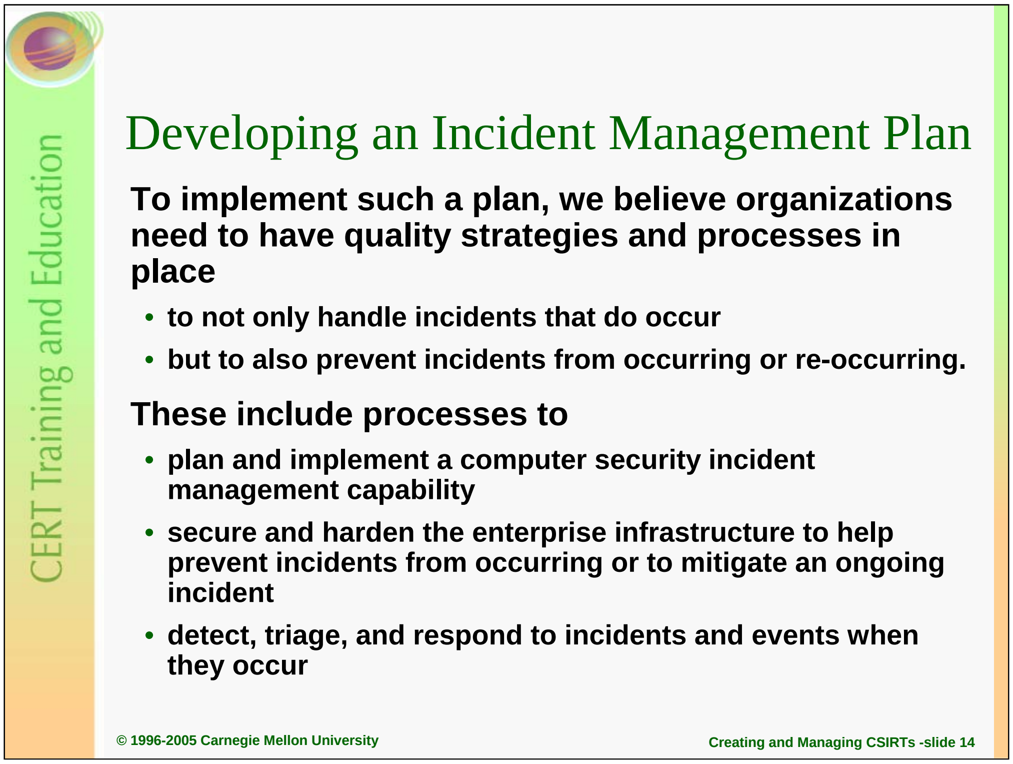
## Process versus Technology

The Announcement function is optional. Arrows indicate information flow.

Creating and Managing CSIRTs -slide 13

As organizations become more complex and incident management capabilities such as CSIRTs become more integrated into organizational business functions, it is clear that incident management is not just the application of technology to resolve computer security events. It is also the development of a plan of action, a set of processes that are consistent, repeatable, of high quality, measurable, and understood within the constituency. 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



CERT Training and Education

## Developing an Incident Management Plan

**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.**

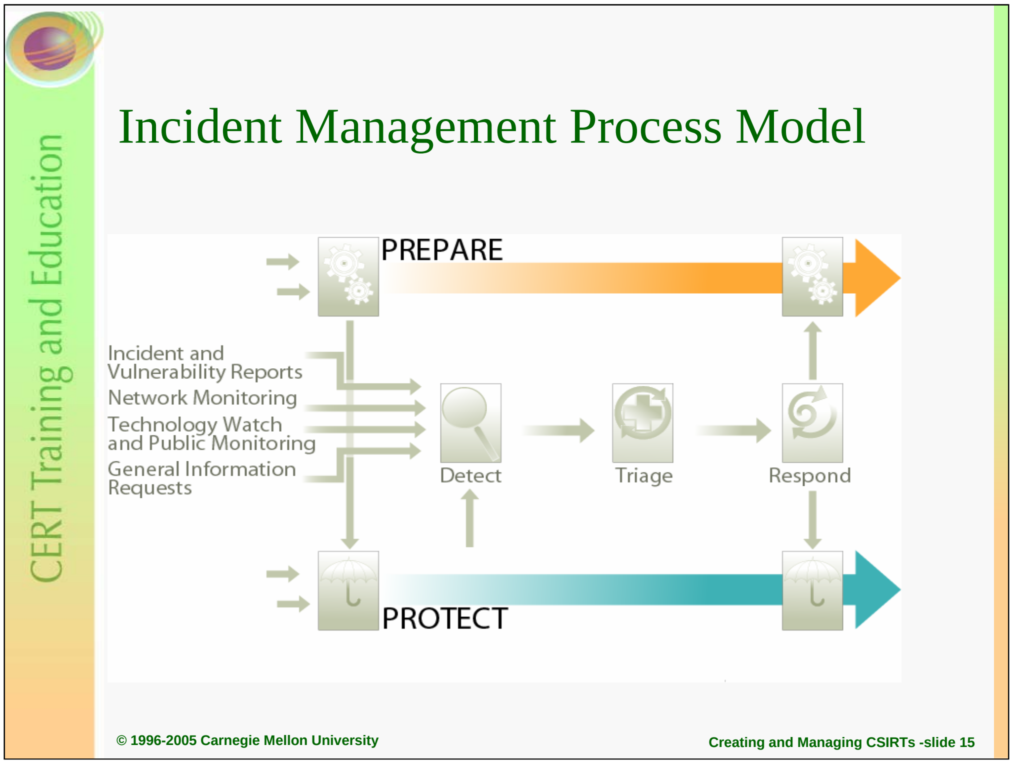
**These include processes to**

- **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**

Creating and Managing CSIRTs -slide 14

The basic principles of such a plan are that Incident management processes are distributed in nature and should

- be enterprise driven
- have defined roles and responsibilities to ensure accountability
- have defined interfaces and communication channels with supporting policies and procedures for coordination across processes and process actors
- be integrated into other business and security management processes



CERT Training and Education

## Incident Management Process Model

PREPARE

Incident and Vulnerability Reports

Network Monitoring

Technology Watch and Public Monitoring

General Information Requests

Detect

Triage

Respond

PROTECT

© 1996-2005 Carnegie Mellon University

Creating and Managing CSIRTs -slide 15

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

To do this we

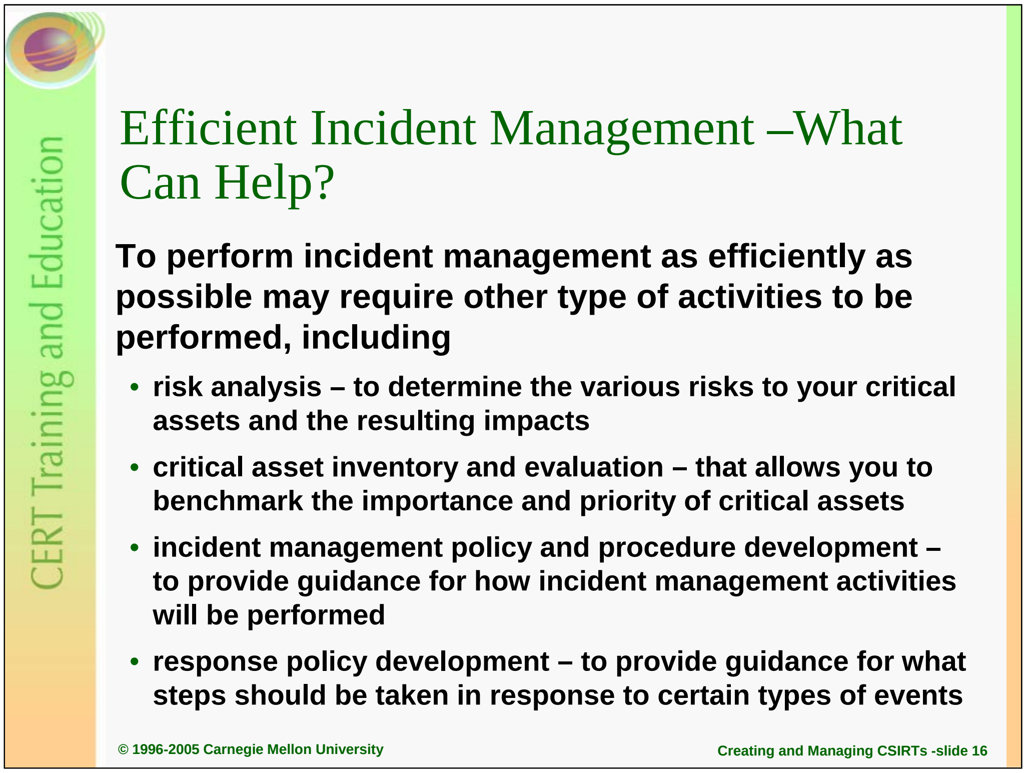
- determined processes
- outlined processes via workflow diagrams
- provided details and requirements of each process

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.



CERT Training and Education

## Efficient Incident Management –What Can Help?

**To perform incident management as efficiently as possible may require other type of activities to be performed, including**

- **risk analysis – to determine the various risks to your critical assets and the resulting impacts**
- **critical asset inventory and evaluation – that allows you to benchmark the importance and priority of critical assets**
- **incident management policy and procedure development – to provide guidance for how incident management activities will be performed**
- **response policy development – to provide guidance for what steps should be taken in response to certain types of events**

Creating and Managing CSIRTs -slide 16

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

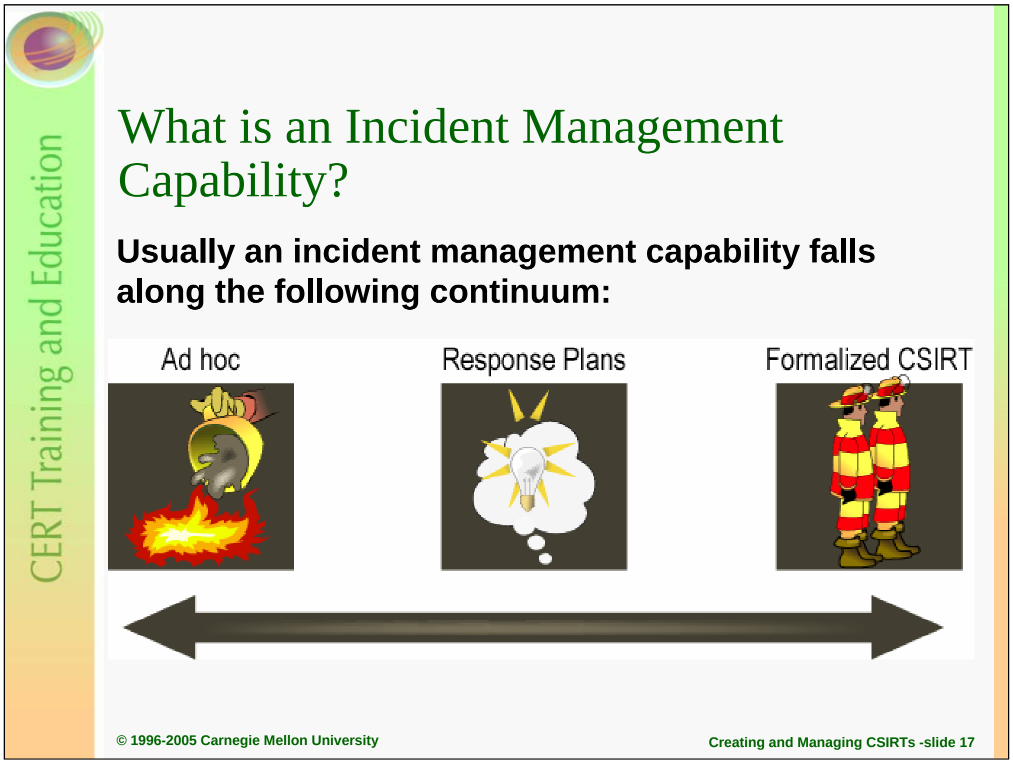
Various types of risk analysis methodologies or industry standards for computer security practices exist. Examples include the following:

- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), information is available at

  http://www.cert.org/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, Information Technology – Guidelines for the Management of IT Security
- ISO 17799, Information Technology – Code of Practice for Information Security Management
- ISO 21827, Maturity Model (SSE-CMM®)
- ISO 15408, Information Technology – Security Techniques -- Evaluation Criteria for IT Security.

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



CERT Training and Education

## What is an Incident Management Capability?

**Usually an incident management capability falls along the following continuum:**

Ad hoc

Response Plans

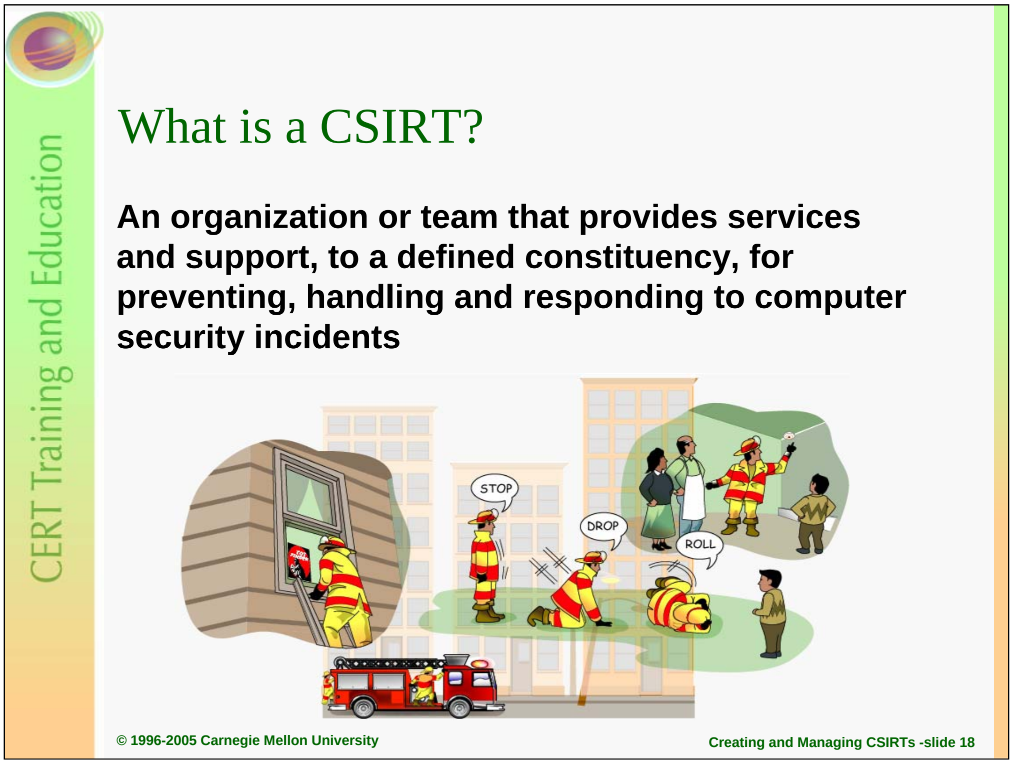
Formalized CSIRT

Creating and Managing CSIRTs -slide 17

An incident management 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. All of these different forms are generically what we referred to as a “CSIRT, a Computer Security Incident Response Team”.

This continuum deals with the structure of the group, not with how well incident management activities are performed. However, the more ad hoc an incident management capability is, the less proactive its services tend to be. Without defined procedures and assigned responsibilities and roles as part of the ad hoc structure, response has the potential to be delayed. That said, many ad hoc groups perform admirably when they have defined processes, assignments, and interfaces.

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.



CERT Training and Education

## What is a CSIRT?

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

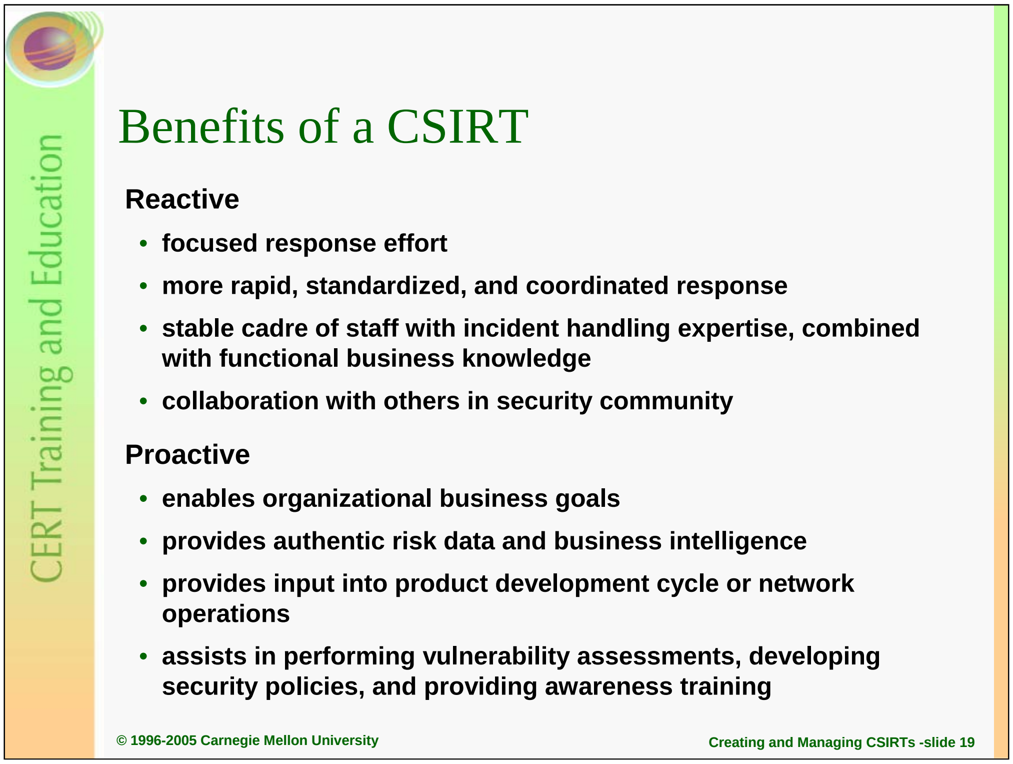
STOP
DROP
ROLL

Creating and Managing CSIRTs -slide 18

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, attack, 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.



CERT Training and Education

# 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**

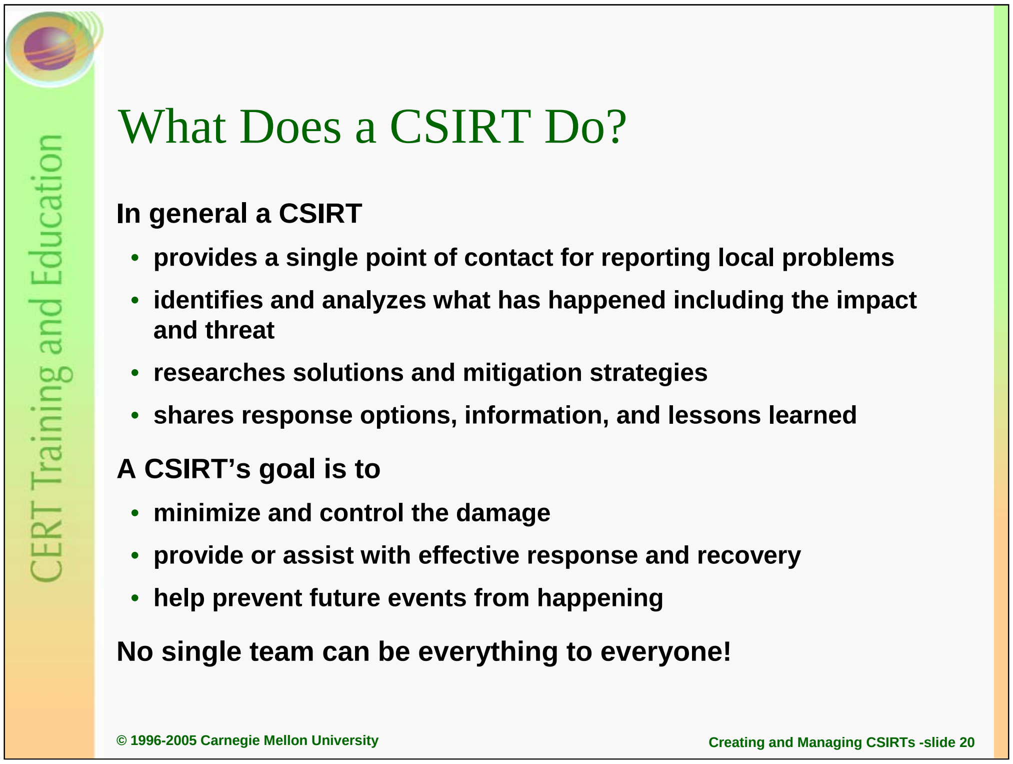
**Proactive**

- **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**

CSIRTs can be on site and able to conduct a rapid response to contain and recover from a computer security incident. CSIRTs may also have familiarity with the compromised systems and therefore be more readily able to coordinate the recovery and propose mitigation and response strategies. Their relationships with other CSIRTs and security organizations can facilitate sharing of response strategies and early alerts to potential problems.

CSIRTs started as “response-oriented” organizations, but have since developed into organizations that work proactively to defend and protect the critical assets of organizations and the Internet community in general. This proactive work includes providing security awareness and education services, influencing policy, and coordinating workshops and information exchanges. It also includes analyzing intruder trends and patterns to create a better understanding of the changing environment so that corresponding prevention, mitigation, and response strategies can be developed and disseminated.

CSIRTs can work with other areas of the organization to ensure new systems are developed and deployed with “security in mind” and in conformance with any site security policies. They can help identify vulnerable areas of the organization and in some cases perform vulnerability assessments and incident detection.



CERT Training and Education

## 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**

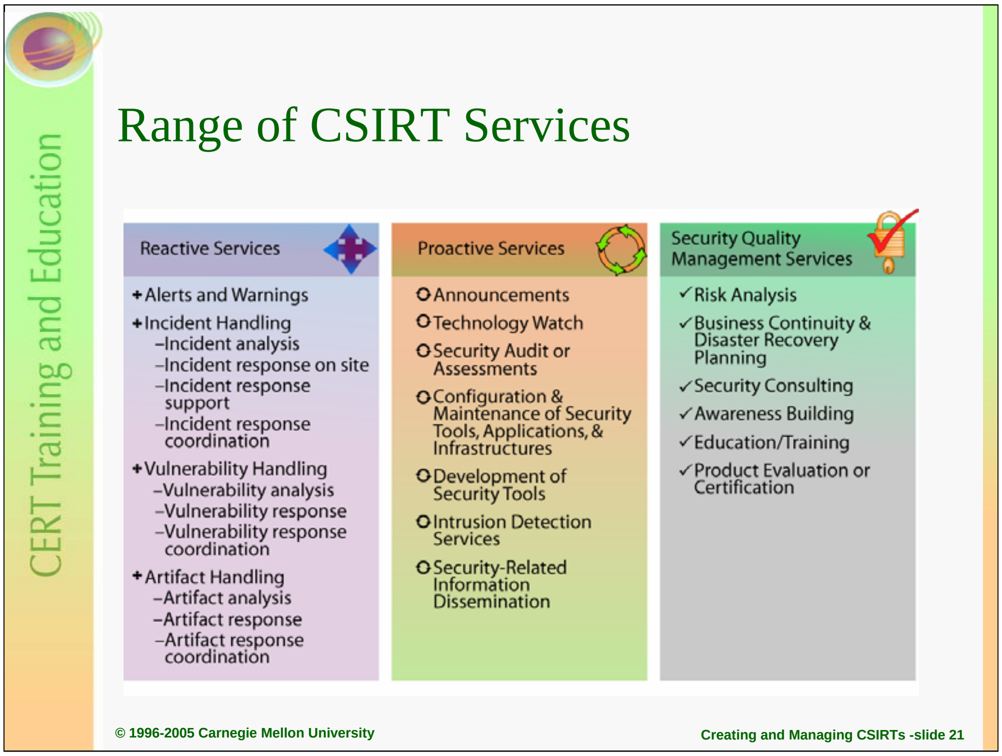
**No single team can be everything to everyone!**

Creating and Managing CSIRTs -slide 20

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.

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?

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.



CERT Training and Education

# Range of CSIRT Services

**Reactive 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

**Proactive Services**

- ○ 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

**Security Quality Management Services**

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

© 1996-2005 Carnegie Mellon University

Creating and Managing CSIRTs -slide 21

Here is an example of the types of services a CSIRT might choose to offer. 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. They can also be found in the online version of this document at:

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

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.

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

**Reactive services.**

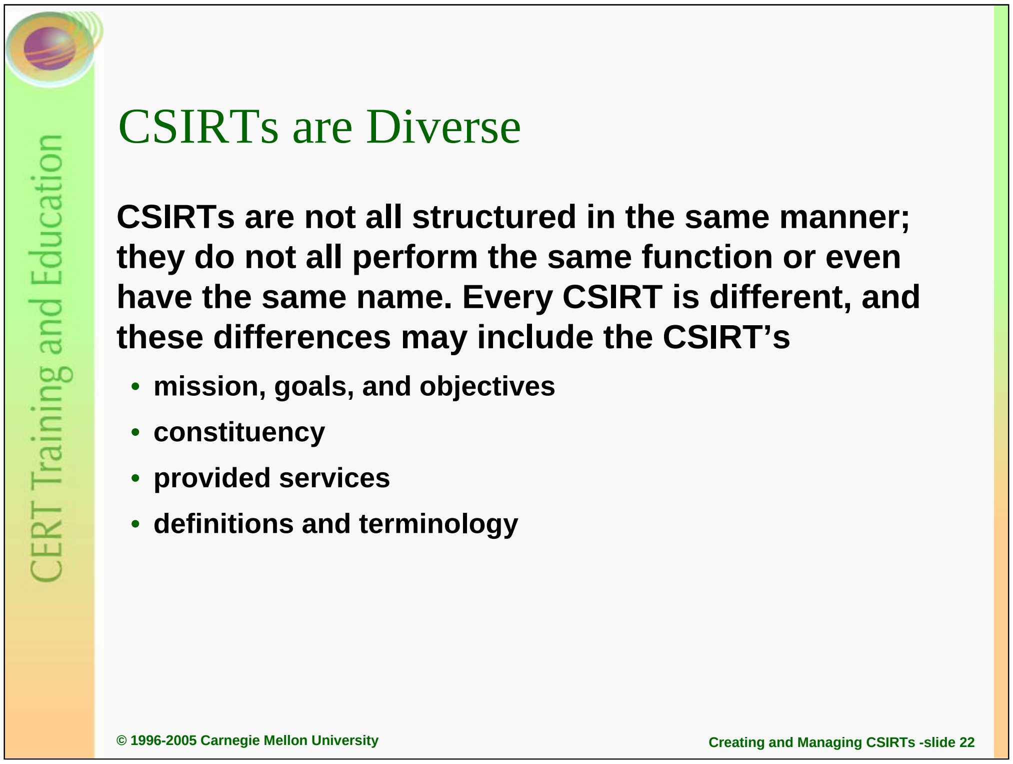
These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, or something that was identified by an intrusion detection or network logging system. Reactive services are the core component of incident handling work.

**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.



CERT Training and Education

## CSIRTs are Diverse

**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**

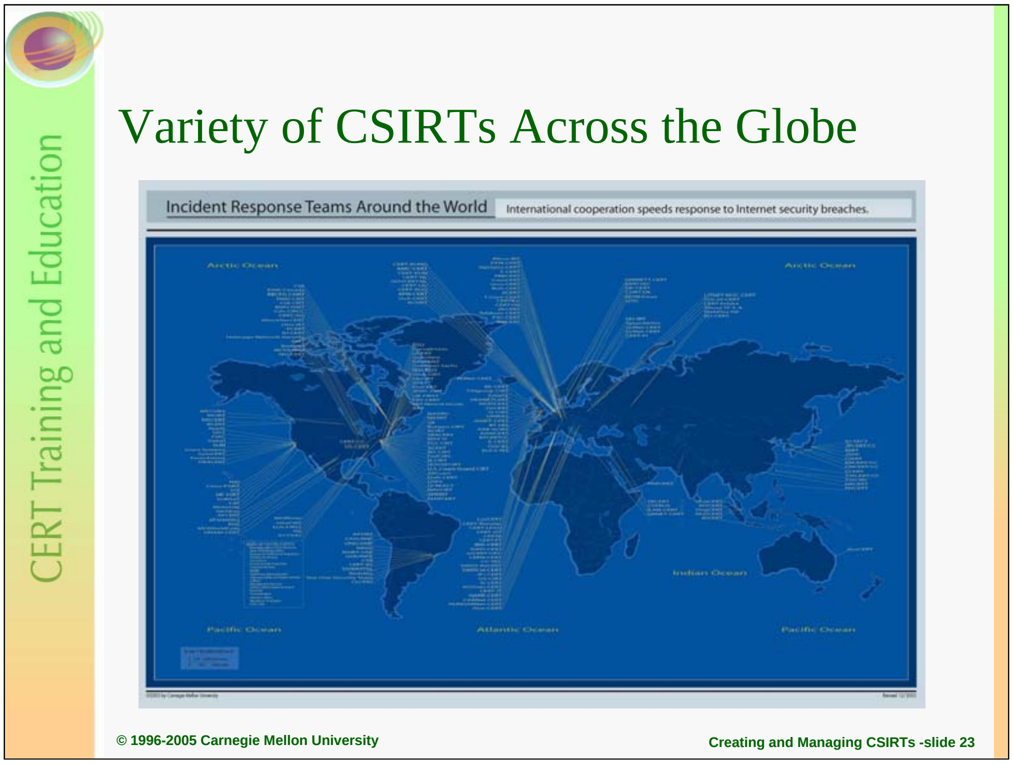
- **mission, goals, and objectives**
- **constituency**
- **provided services**
- **definitions and terminology**

Creating and Managing CSIRTs -slide 22

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 can be very different, but basically all of the acronyms and titles below are organizations performing similar types of functions. We consider all of the following titles to be a representation of the same type of organization, a CSIRT.

| | |
|---|---|
| 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 |



CERT Training and Education

## Variety of CSIRTs Across the Globe

Incident Response Teams Around the World
International cooperation speeds response to Internet security breaches.
Arctic Ocean
Arctic Ocean
Indian Ocean
Pacific Ocean
Atlantic Ocean
Pacific Ocean

Creating and Managing CSIRTs -slide 23

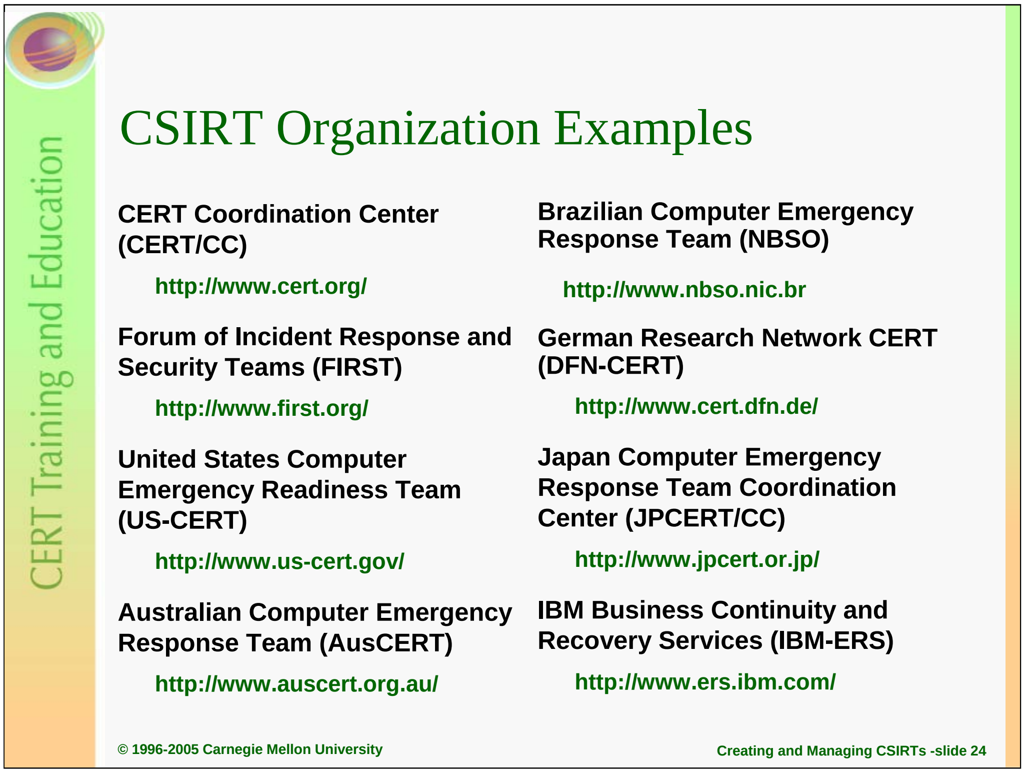
CSIRTs come in all shapes and sizes and serve diverse constituencies. Some CSIRTs, such as the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), support an entire country. Other CSIRTs may provide support to a particular university such as Oxford, a commercial organization such 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 CSIRTs - provide incident handling services to their parent organization; this could be a CSIRT for a bank, a university, or a federal agency.
- Coordination Centers – coordinate and facilitate the handling of incidents across various CSIRTs, or for a particular country, state, region, province, research network, or other such entity. 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/



CERT Training and Education

# CSIRT Organization Examples

**CERT Coordination Center (CERT/CC)**

http://www.cert.org/

**Forum of Incident Response and Security Teams (FIRST)**

http://www.first.org/

**United States Computer Emergency Readiness Team (US-CERT)**

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

**Australian Computer Emergency Response Team (AusCERT)**

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

**Brazilian Computer Emergency Response Team (NBSO)**

http://www.nbso.nic.br

**German Research Network CERT (DFN-CERT)**

http://www.cert.dfn.de/

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

http://www.jpcert.or.jp/

**IBM Business Continuity and Recovery Services (IBM-ERS)**

http://www.ers.ibm.com/

Creating and Managing CSIRTs -slide 24

CSIRTs come in all “shapes and sizes” and serve broadly diverse constituencies.

Some CSIRTs support a country like the JP-CERT/CC, others may provide assistance to a particular region; and yet others may provide support to a particular university or commercial organization.

Here are some examples of various types of CSIRTs. These examples contain teams from various commercial, governmental, and educational areas across the world.

FIRST is the international forum of incident response and security teams. Established in 1990, FIRST is a coalition that brings together a variety of security teams and computer security incident response teams from government, commercial, and academic organizations.

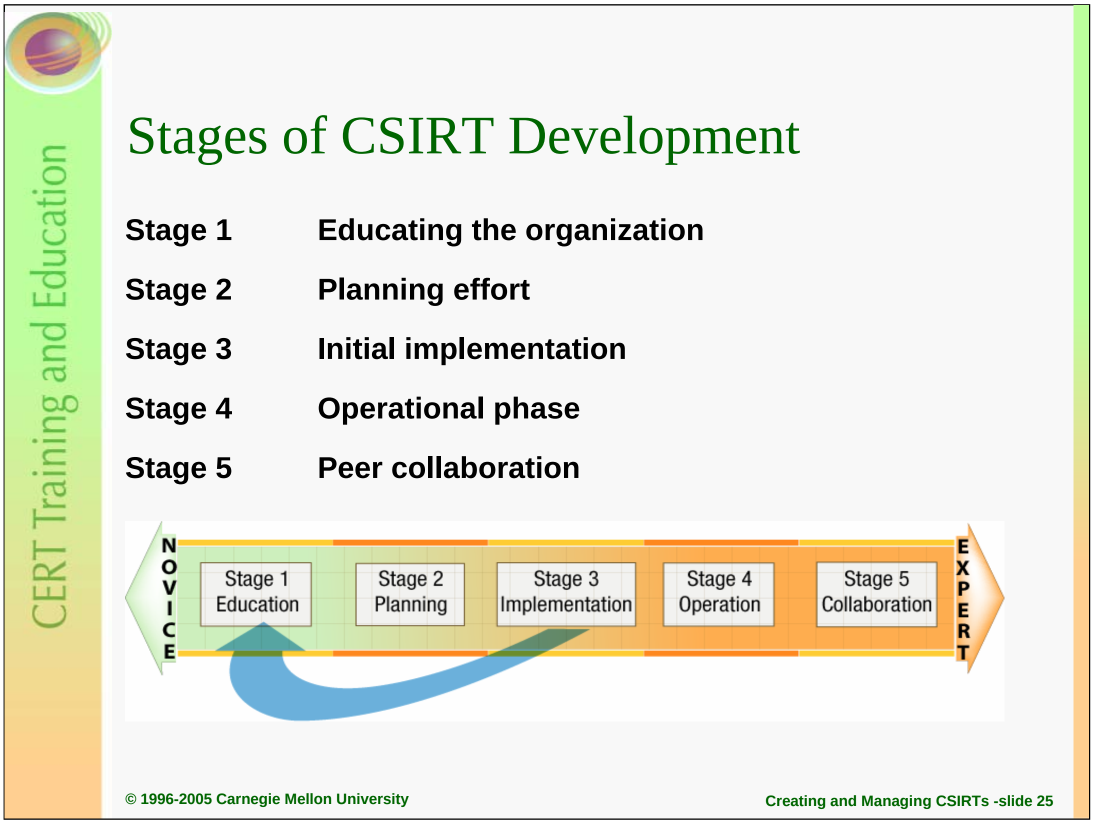
Attending the yearly FIRST conferences can be a way for a new or existing team to learn more about techniques and strategies for providing a response capability. It is also a good way to make contact with established teams.

You can learn more about FIRST via their Web page at

http://www.first.org/

If you would like to become a member, please look at

http://www.first.org/docs/joining.first.html



CERT Training and Education

## Stages of CSIRT Development

| | |
|---|---|
| **Stage 1** | **Educating the organization** |
| **Stage 2** | **Planning effort** |
| **Stage 3** | **Initial implementation** |
| **Stage 4** | **Operational phase** |
| **Stage 5** | **Peer collaboration** |

NOVICE
Stage 1 Education
Stage 2 Planning
Stage 3 Implementation
Stage 4 Operation
Stage 5 Collaboration
EXPERT

Creating and Managing CSIRTs -slide 25

This slide represents the stages in a CSIRT’s development according to the CERT/CC CSIRT Development Team.

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

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 is built and begins to provide services. It already possesses an identified constituency, mission and services, initial staff and training, draft standard operating procedures (SOPs), and a secure infrastructure.

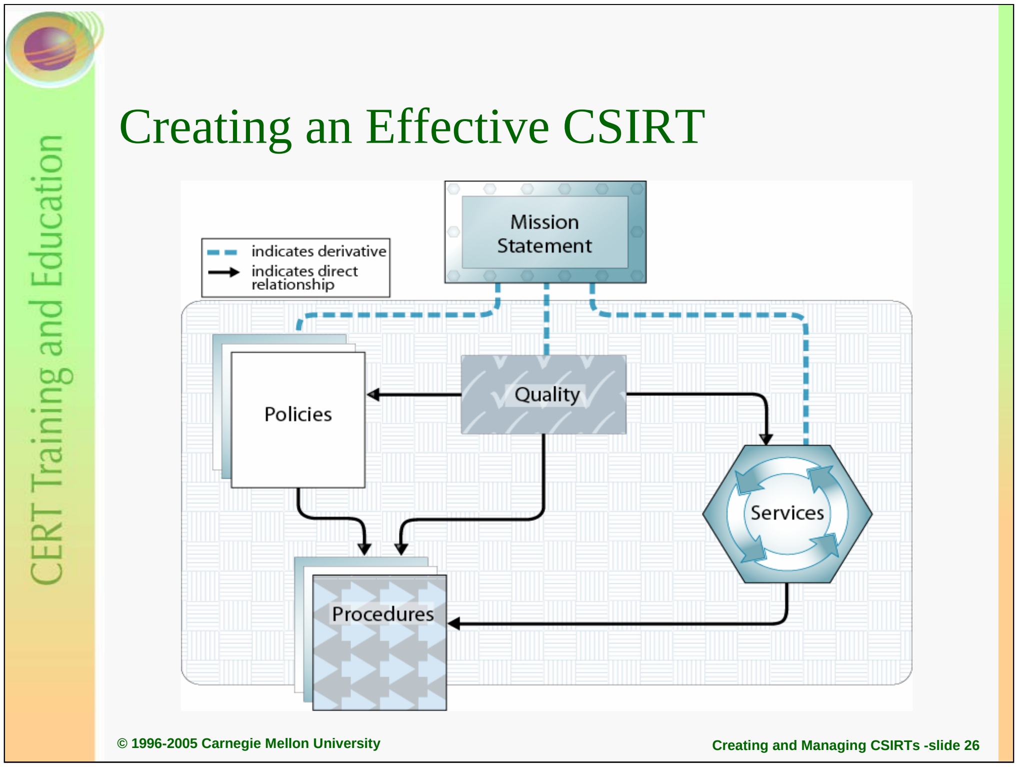
In **Stage 4**, the CSIRT is handling incidents and has been operational for six months to one year.

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. It is a peer collaborator with other CSIRTs.

It is important to realize that you may be at a more advanced stage but still need to step back and revisit some of the early stages to validate that you are addressing all the right issues.

Where would you place yourself (and your CSIRT) on this continuum?

Have you handled computer security incidents before?



CERT Training and Education

## Creating an Effective CSIRT

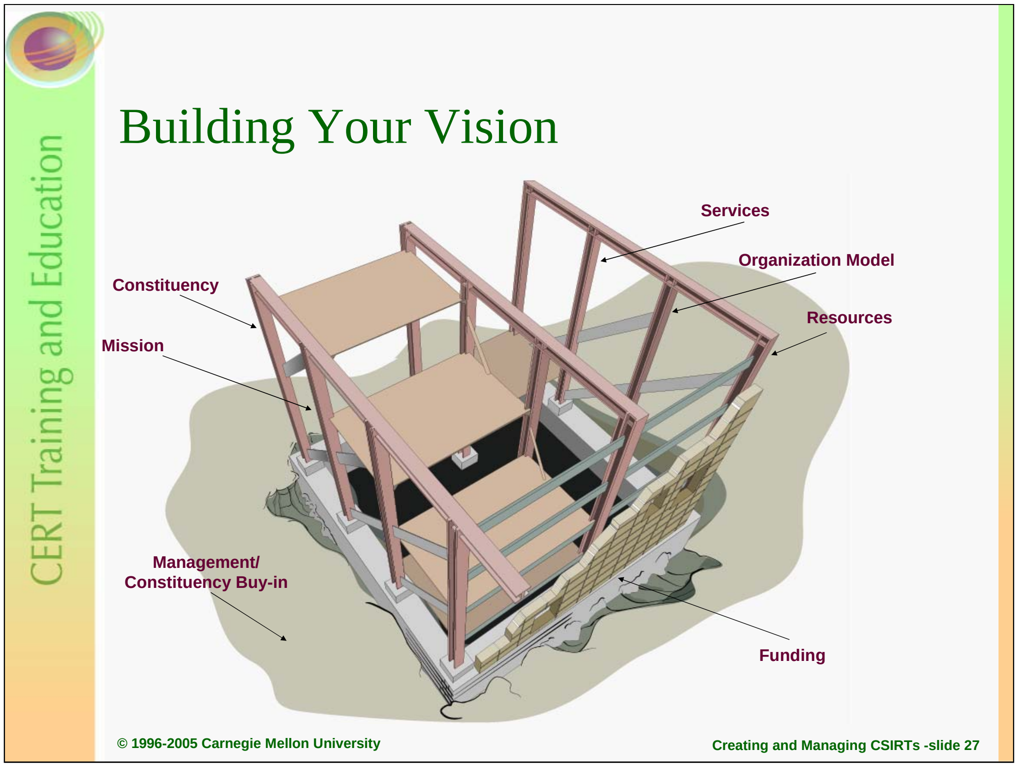
© 1996-2005 Carnegie Mellon University

Creating and Managing CSIRTs -slide 26

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.



CERT Training and Education

## Building Your Vision

© 1996-2005 Carnegie Mellon University

Creating and Managing CSIRTs -slide 27

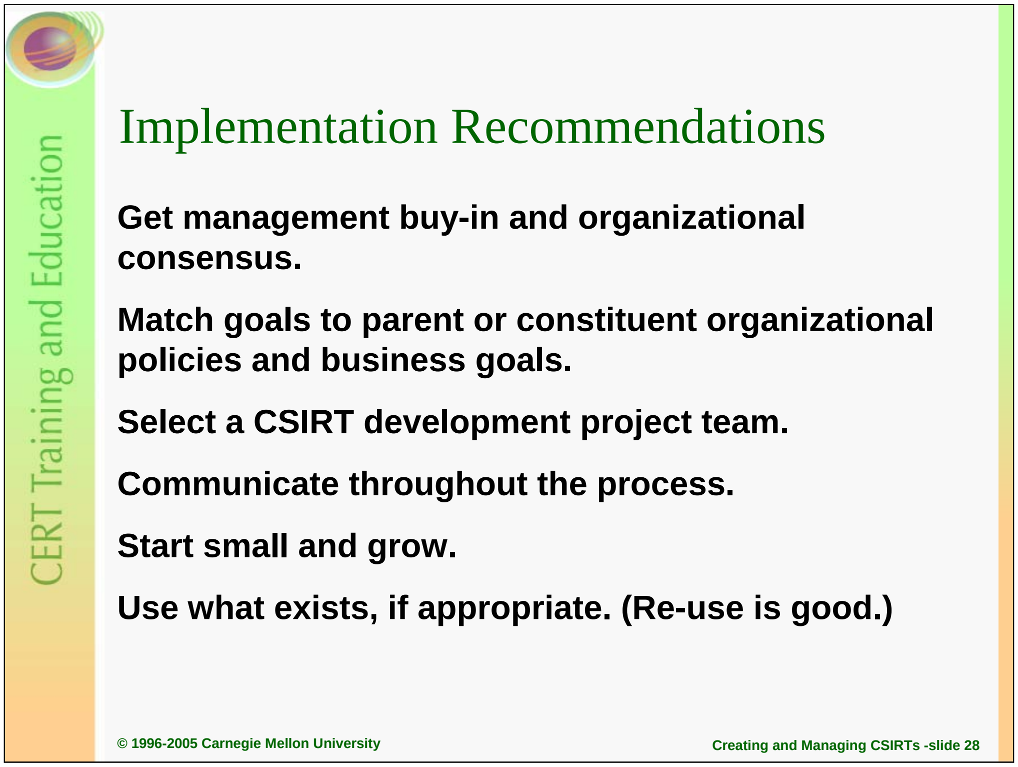
The basic components or building blocks of your CSIRT framework make up your CSIRT vision. These components include:

- 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.

During this session we will focus on identifying your constituency, developing your mission, and finding alternative funding strategies. Sessions later in the material will address services, organizational and reporting structures, authority, and CSIRT resources.



CERT Training and Education

## 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. (Re-use is good.)

Creating and Managing CSIRTs -slide 28

A CSIRT planning team project leader with authority for decision making should also 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.

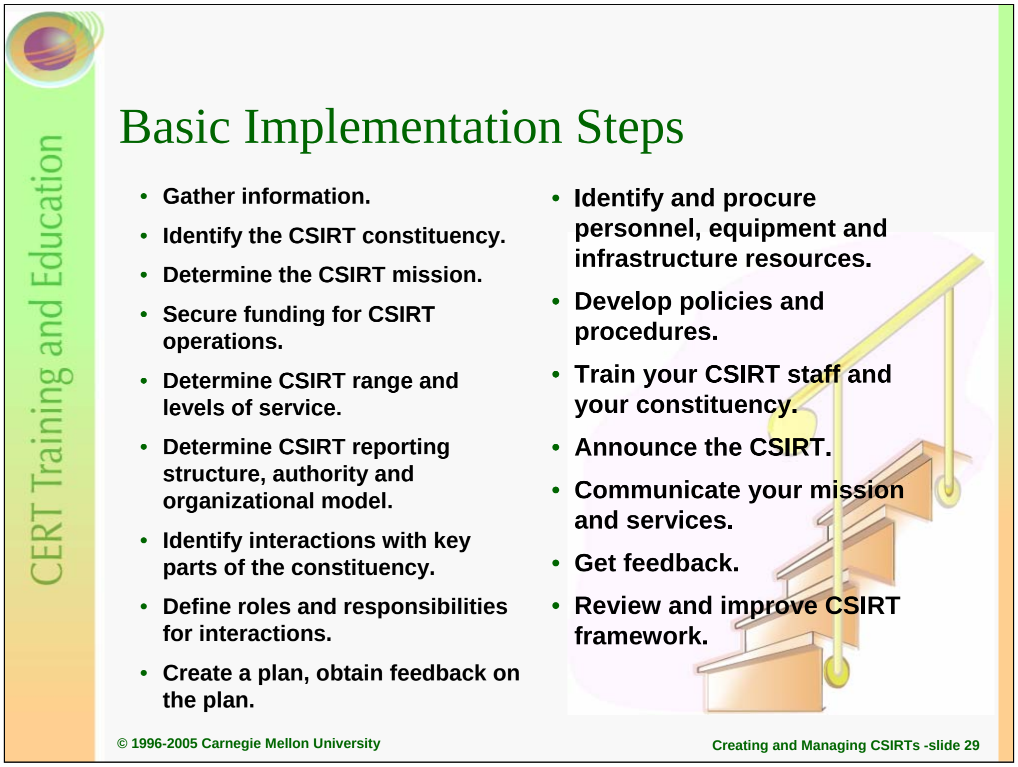
Management buy-in must include providing personnel, time, and funding.

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.



CERT Training and Education

## Basic Implementation Steps

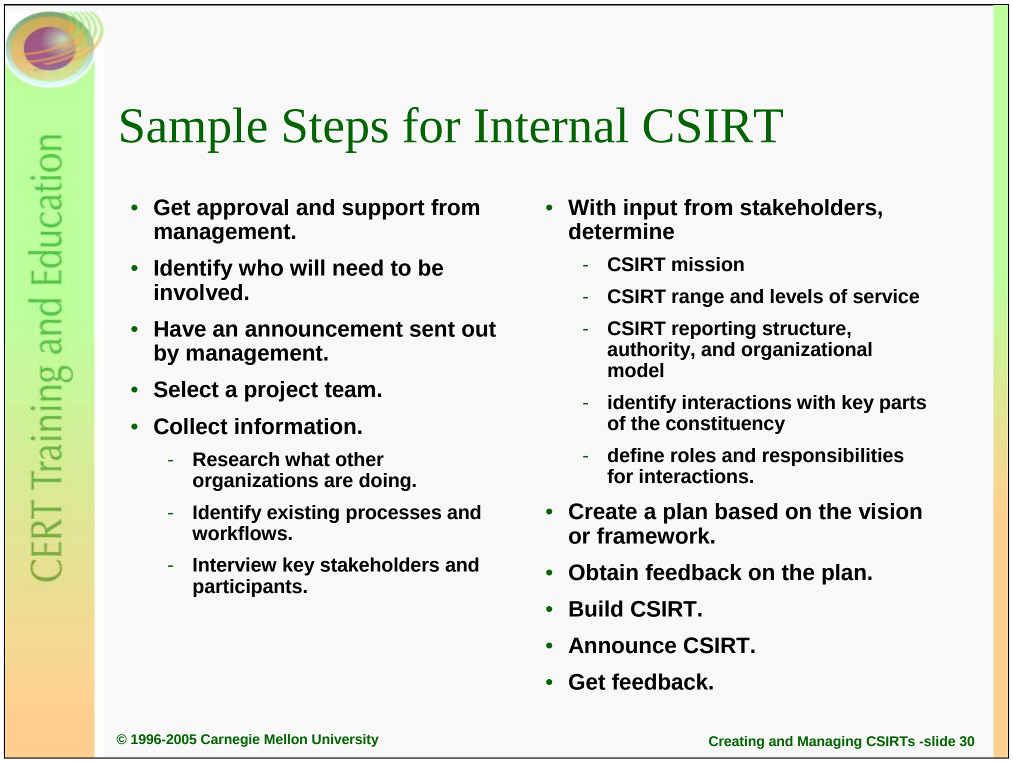
- Gather information.
- Identify the CSIRT constituency.
- Determine the CSIRT mission.
- Secure funding for CSIRT operations.
- Determine CSIRT range and levels of service.
- Determine CSIRT reporting structure, authority and organizational model.
- Identify interactions with key parts of the constituency.
- Define roles and responsibilities for interactions.
- Create a plan, obtain feedback on the plan.
- Identify and procure personnel, equipment and infrastructure resources.
- Develop policies and procedures.
- Train your CSIRT staff and your constituency.
- Announce the CSIRT.
- Communicate your mission and services.
- Get feedback.
- Review and improve CSIRT framework.

Creating and Managing CSIRTs -slide 29

Remember that it is critically important to get both management and constituency buy-in and support.

Internal and external communications methods are necessary to let constituents and other stakeholders understand the implementation and also to provide mechanisms for review of and feedback on the plan.

When the CSIRT is ready to become operational, it should be announced.  All of the constituency should understand what their interaction with the CSIRT should be - including when and how to contact and report anomalies and incident activity to the CSIRT.



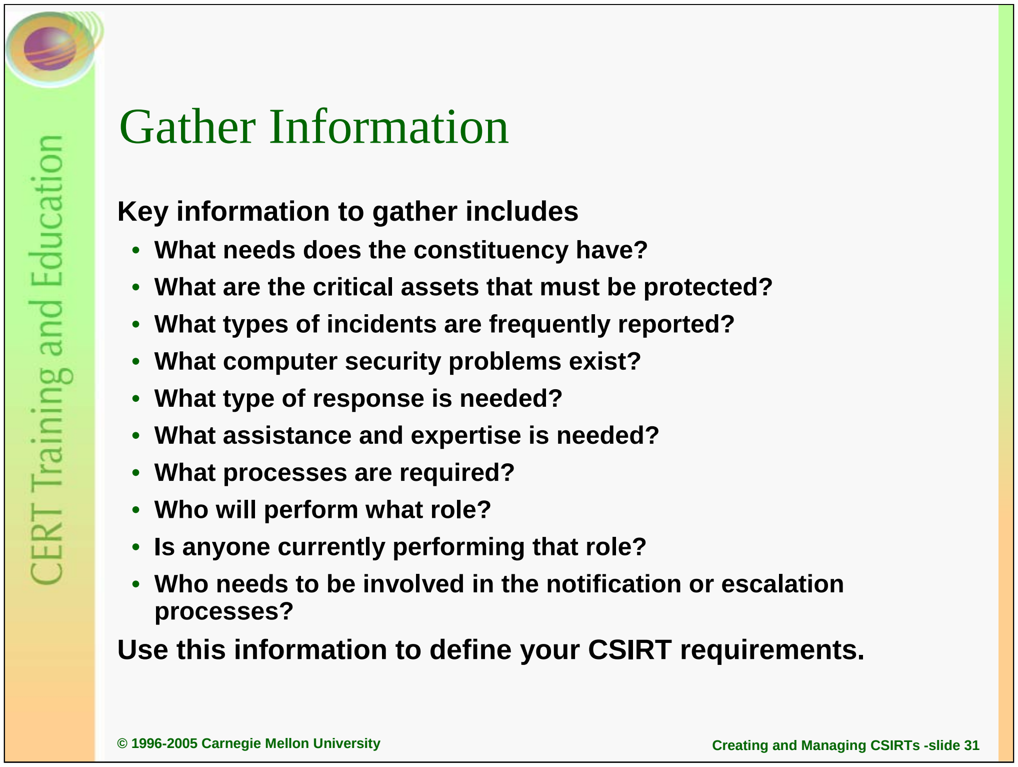
CERT Training and Education

## Sample Steps for Internal CSIRT

- Get approval and support from management.
- Identify who will need to be involved.
- Have an announcement sent out by management.
- Select a project team.
- Collect information.
  - Research what other organizations are doing.
  - Identify existing processes and workflows.
  - Interview key stakeholders and participants.
- With input from stakeholders, determine
  - CSIRT mission
  - CSIRT range and levels of service
  - CSIRT reporting structure, authority, and organizational model
  - identify interactions with key parts of the constituency
  - define roles and responsibilities for interactions.
- Create a plan based on the vision or framework.
- Obtain feedback on the plan.
- Build CSIRT.
- Announce CSIRT.
- Get feedback.

Sample Planning Steps for an internal CSIRT within an organization:

- get approval and support for the CSIRT planning and implementation project; including funding, resources, and time for project team and others on staff to participate
- identify who will need to be involved in the planning and implementation process
- have an announcement sent out by upper management (CEO or equivalent or the CIO or equivalent) to the organization explaining that a CSIRT is being planned and the basic process that will be followed to do the implementation
- select a project team
- research what other organizations are doing to create a CSIRT and what best practices or guides exist
- collect information from existing organization charts, network topologies, security policies, institutional rules and regulations, existing disaster recovery or incident response plans, existing business continuity plans, and critical system and network asset inventories
- interview business managers, information technology staff and managers, and end-users to understand the current process for handling computer security incidents
- identify who is performing the following functions: firewall operation and maintenance, intrusion detection, other network or host monitoring, vulnerability assessments or scanning, penetration testing, patch maintenance and operating system updates
- interview business mangers, information technology staff, end users, and representatives from legal, human resources, and public relations to determine what needs these areas have regarding incident management and response
- with input from all stakeholders, define the vision or framework for the CSIRT, including: CSIRT constituency, mission, authority, services, organizational model and needed staff, equipment, and infrastructure
- create a plan based on the vision and framework and make it available within the organization for feedback and comments
- update the plan with any needed changes based on feedback



CERT Training and Education

# Gather Information

Key information to gather includes

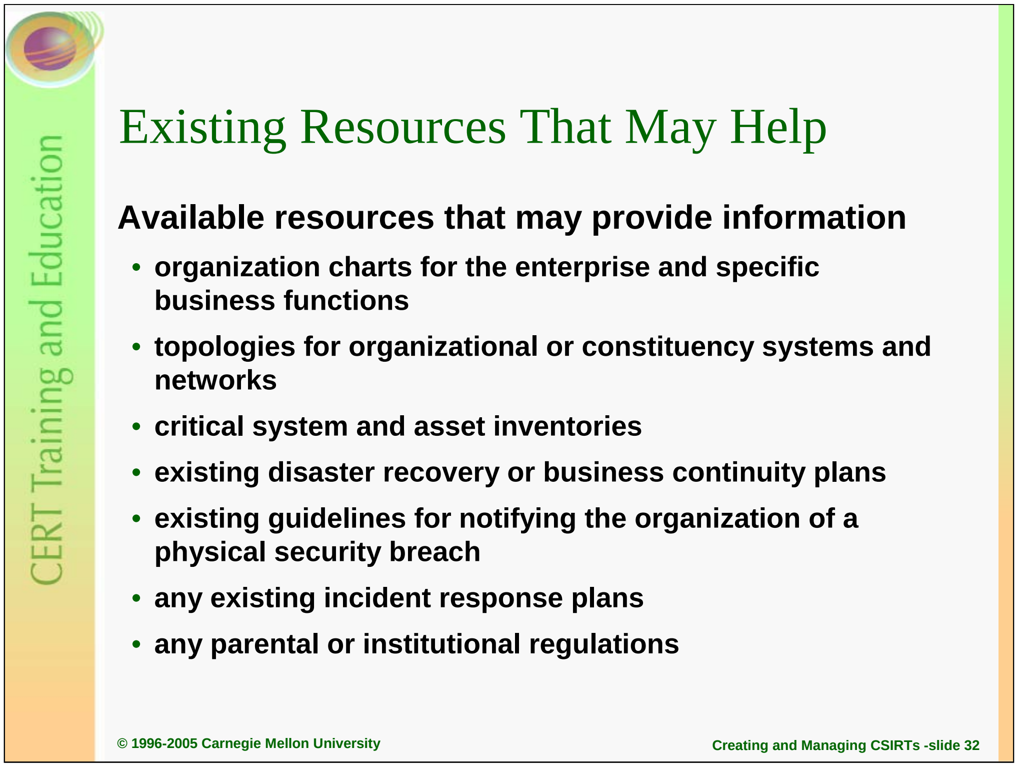
- What needs does the constituency have?
- What are the critical assets that must be protected?
- What types of incidents are frequently reported?
- What computer security problems exist?
- What type of response is needed?
- What assistance and expertise is needed?
- What processes are required?
- Who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

Use this information to define your CSIRT requirements.

Creating and Managing CSIRTs -slide 31

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. Check out 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/CC CSIRT Development Web page: http://www.cert.org/csirts/Creating-A-CSIRT.html



CERT Training and Education

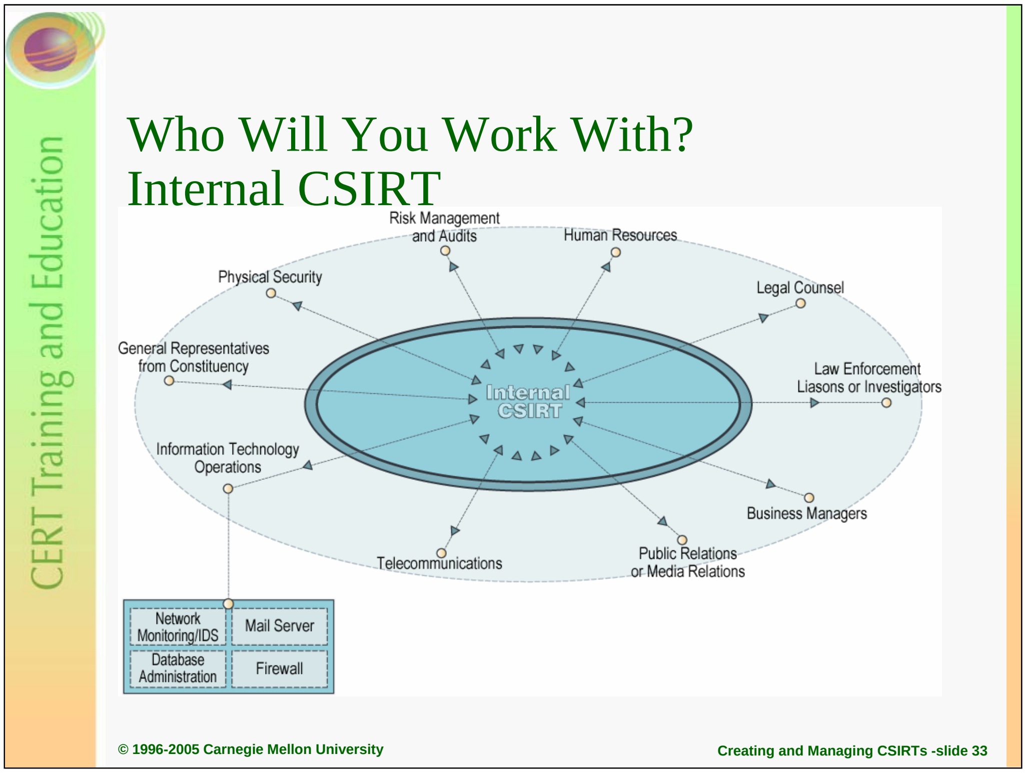
## Existing Resources That May Help

**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**

Many of these resources may not be available or many not exist. 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.



CERT Training and Education

## Who Will You Work With? Internal CSIRT

Internal CSIRT

Risk Management and Audits

Human Resources

Physical Security

Legal Counsel

General Representatives from Constituency

Law Enforcement Liasons or Investigators

Information Technology Operations

Business Managers

Telecommunications

Public Relations or Media Relations

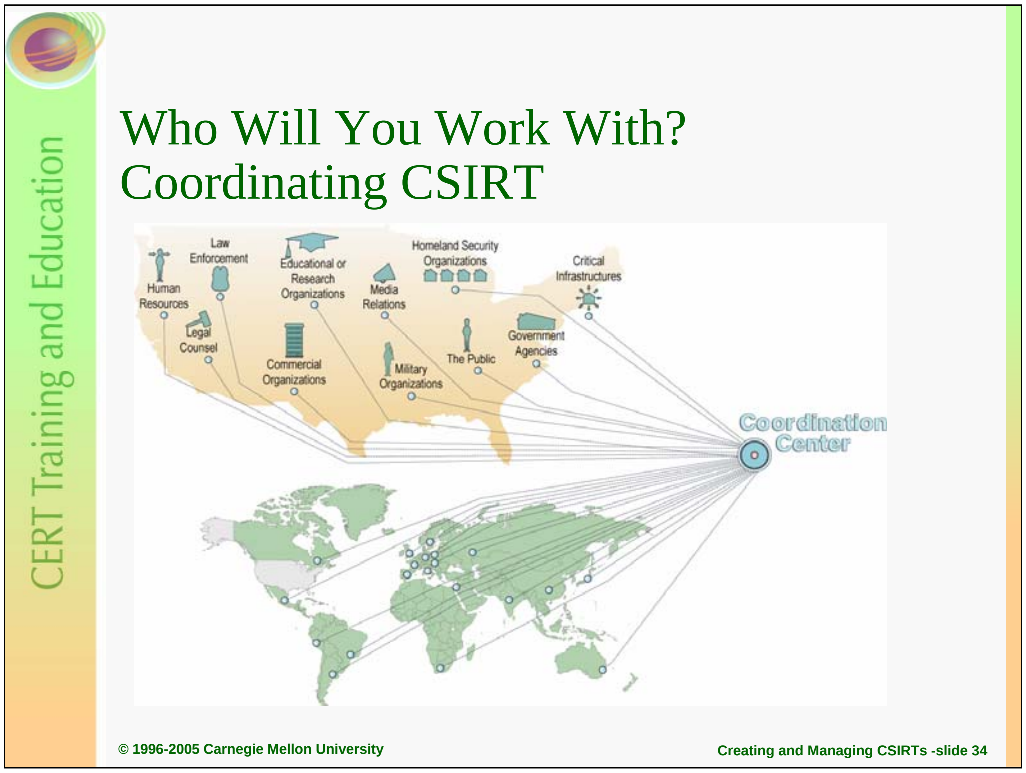
| | |
|---|---|
| Network Monitoring/IDS | Mail Server |
| Database Administration | Firewall |

Creating and Managing CSIRTs -slide 33

Incident Handling is not a self-contained process. Relationships, communication channels, data sharing agreements, and policies and procedures must be established across the organization. For an internal team, this includes

- Business managers. They need to understand what the CSIRT is and how it can help support their business processes. Agreements must be made concerning the CSIRT’s authority over business systems and who will make decisions if critical business systems must be disconnected from the network or shut down.
- Representatives from IT. How will the IT staff and the CSIRT interact? What actions will be taken by IT staff and what actions are taken by CSIRT members? What information can the IT staff provide to the CSIRT and what information the CSIRT can provide to the IT team? What roles and authority do each have?
- Representatives from the legal department. When and how is the legal department involved in incident response efforts?
- Representatives from human resources. They will need to be involved in developing policies and procedures for removing internal employees found engaging in unauthorized or illegal computer activity.
- Representatives from public relations. They must be prepared to handle any media inquiries and help develop information disclosure policies and practices.
- Any existing security groups, including physical security. The CSIRT will need to exchange information with these groups about computer incidents and may share responsibility with them for resolving issues involving computer or data theft.
- Audit and risk management specialists. They can help develop threat metrics and risks to constituency systems.
- Any law enforcement liaisons or investigators. They will understand how the team should work with law enforcement, when to contact them, and who will do the investigations or even forensic analysis.
- General representatives from the constituency. They can provide insight into their needs and requirements.

Other established communications channels are needed with your ISP and any software or hardware vendors, other CSIRTs or external security requirements.



CERT Training and Education

# Who Will You Work With? Coordinating CSIRT

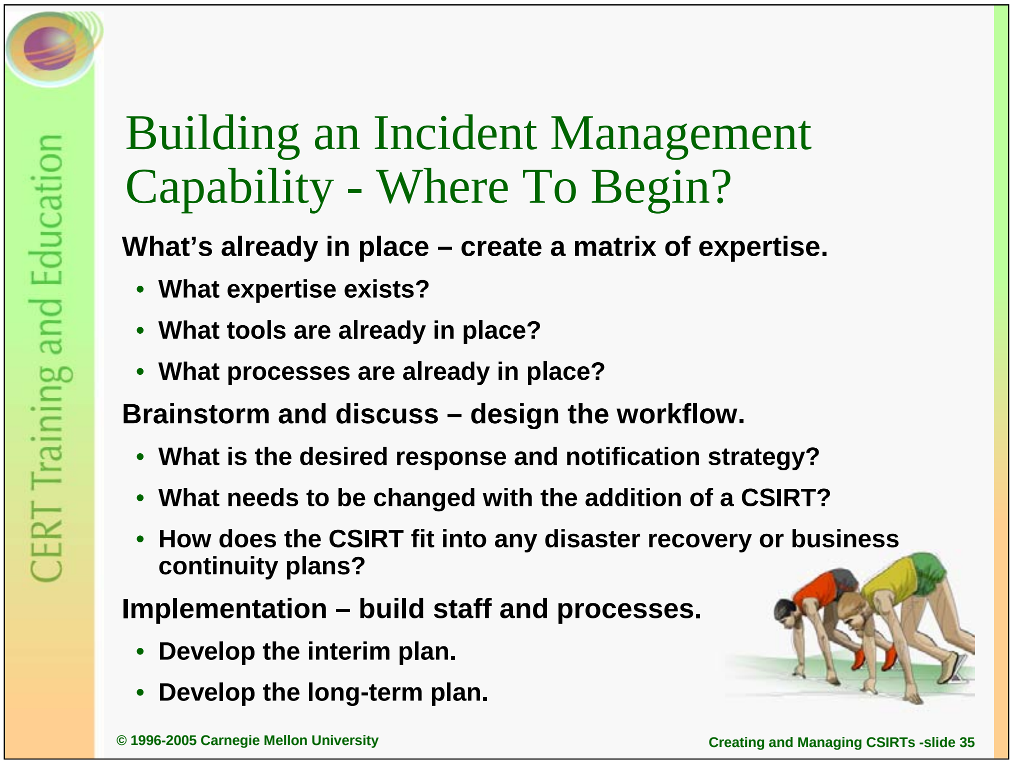
Creating and Managing CSIRTs -slide 34

For teams that serve as a coordination center or support a state, national, provincial or similar government entity constituency – it may be difficult to determine what relationships with the participating organizations should be established.

The CSIRT may only deal with particular organizations such as

- government organizations
- military organizations
- critical infrastructures
- business organizations

Or it may accept reports from and disseminate information to the public, it all depends on the defined mission, constituency, and services of the CSIRT.



CERT Training and Education

## Building an Incident Management Capability - Where To Begin?

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

- **What expertise exists?**
- **What tools are already in place?**
- **What processes 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?**

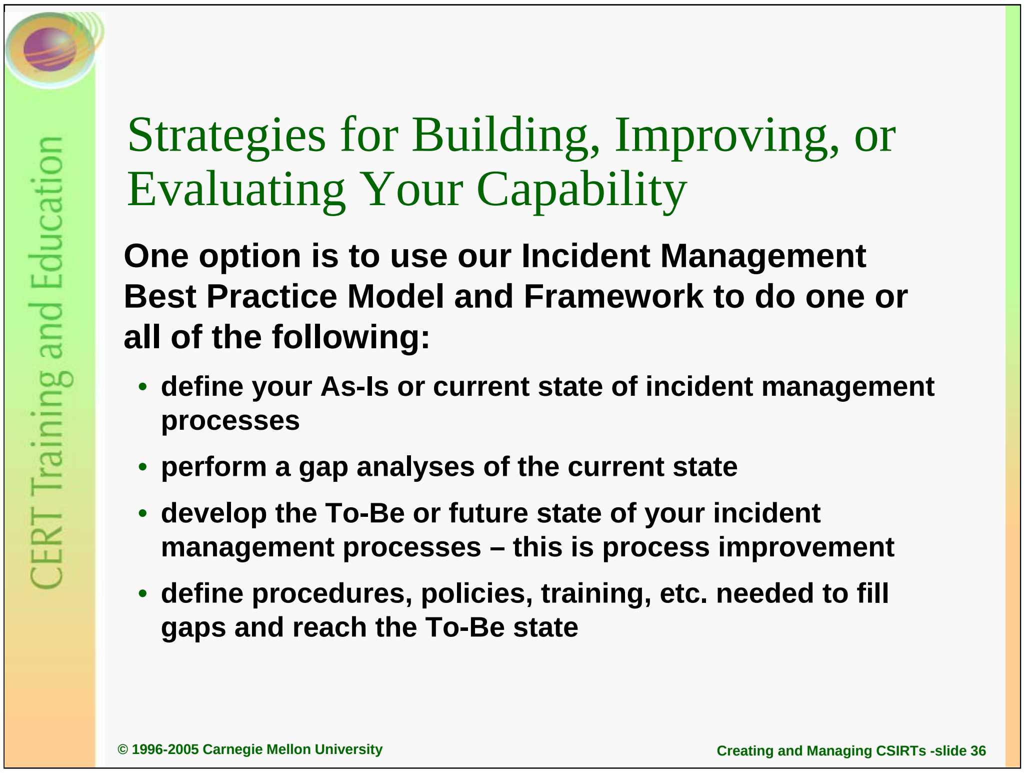
**Implementation – build staff and processes.**

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

Creating and Managing CSIRTs -slide 35

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?

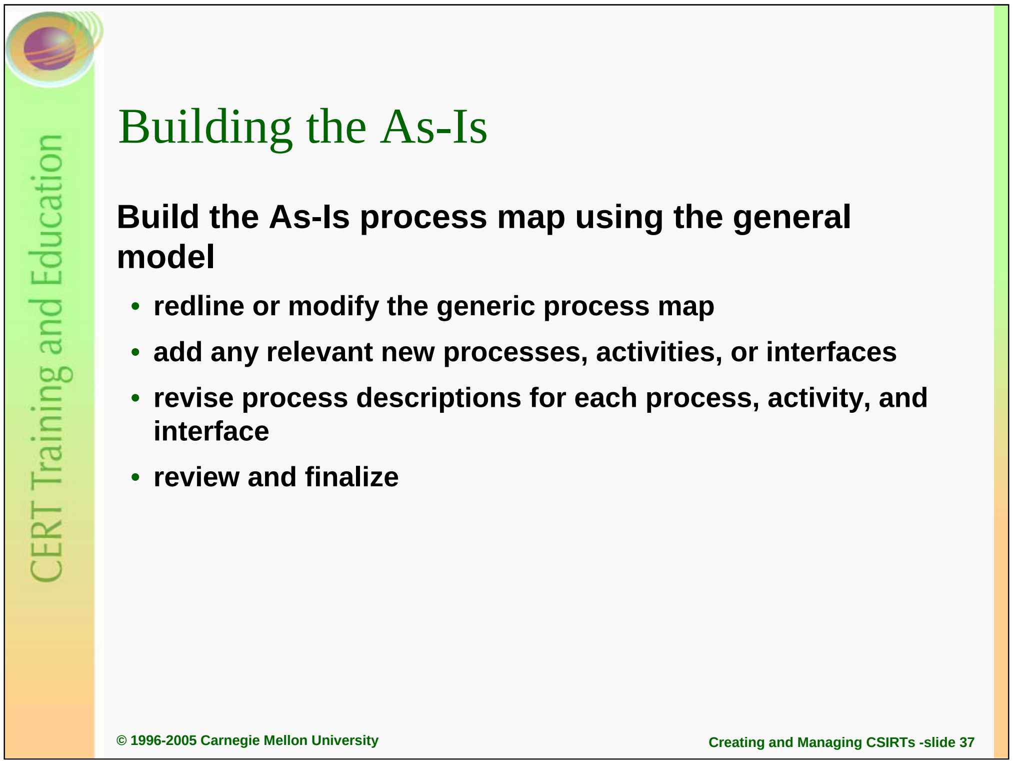


CERT Training and Education

## Strategies for Building, Improving, or Evaluating Your Capability

**One option is to use our Incident Management Best Practice Model and Framework to do one or all of the following:**

- **define your As-Is or current state of incident management processes**
- **perform a gap analyses of the current state**
- **develop the To-Be or future state of your incident management processes – this is process improvement**
- **define procedures, policies, training, etc. needed to fill gaps and reach the To-Be state**


CERT Training and Education

## Building the As-Is

**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**

© 1996-2005 Carnegie Mellon University

Creating and Managing CSIRTs -slide 37

To do this you would need to meet with representatives from the organization and identify who is currently performing the Protect, Detect, Triage, and Respond processes and subprocesses.

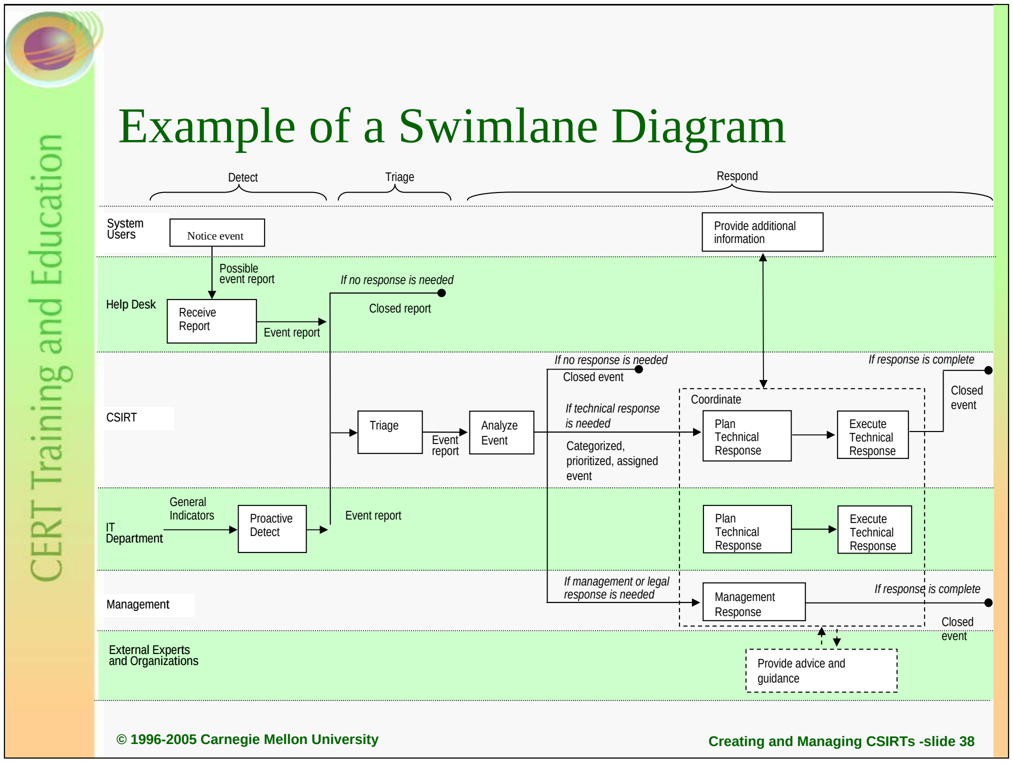
You can accomplish this by doing observations, using surveys, doing interviews and reviewing existing documentation such as policies, procedures, and guidelines.

Once you've done this you can create a process workflow to diagram who is performing these functions and how information is passed from one group to another.

One way to diagram this information is using a swimlane diagram.

Types of information to capture for each process will include:

- Mission/Objectives of the process
- Triggers for initiation
- Completion Criteria
- Policies and Rules (that affect or impact the process)
- General Requirements (for carrying out the process in a successful manner, such as appropriate training and equipment, appropriate documentation of actions, appropriate training of involved staff)
- Inputs and Outputs to the process
- Subprocesses and Subprocess requirements
- Written procedures that are used during the process or detail the process steps
- Key people (who perform the process)
- Technology (used to perform the process)



# Example of a Swimlane Diagram

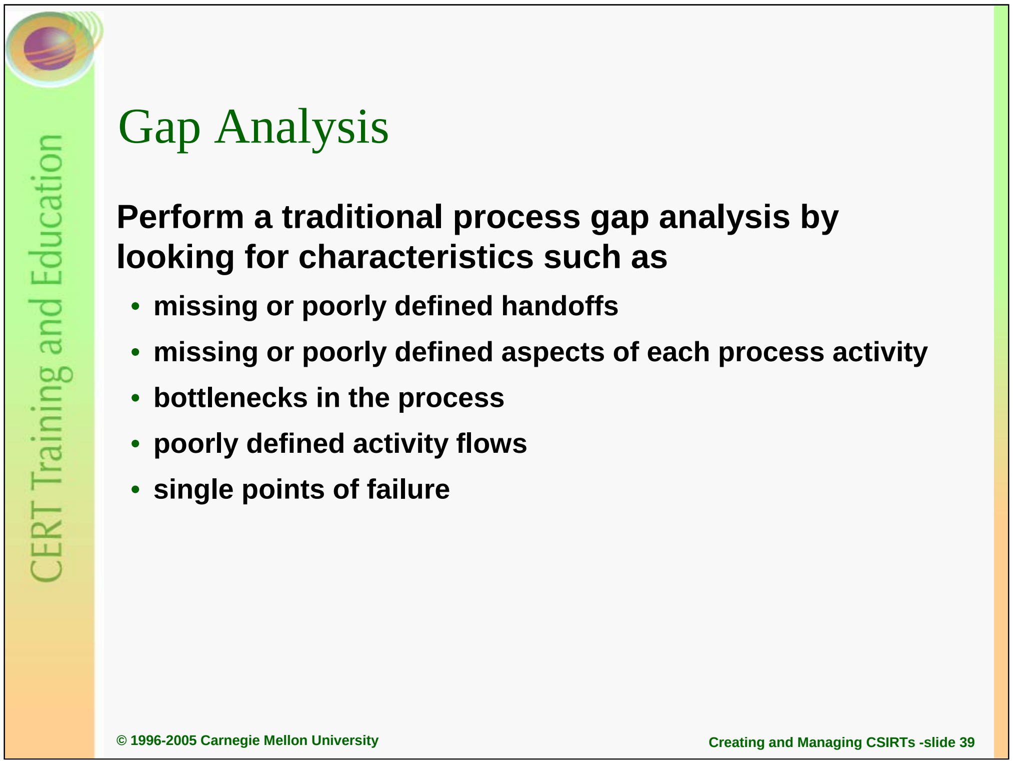
© 1996-2005 Carnegie Mellon University

Creating and Managing CSIRTs -slide 38

Example of a Swimlane Diagram.

The process workflow diagrams and descriptions in the Best Practice Incident Management process model are very generic in nature. As organization customizes the processes to match their own situation, they would begin to add in 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. This type of diagram is called a “swimlane” diagram.


CERT Training and Education

## Gap Analysis

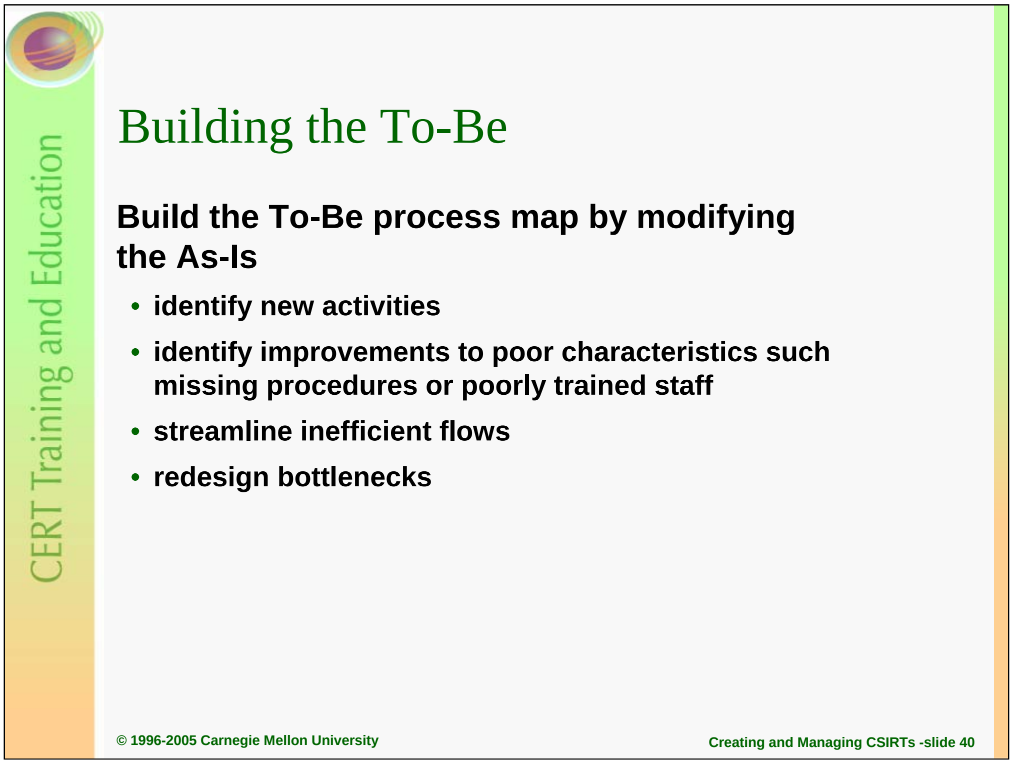
**Perform a traditional process gap analysis by looking for characteristics such as**

- **missing or poorly defined handoffs**
- **missing or poorly defined aspects of each process activity**
- **bottlenecks in the process**
- **poorly defined activity flows**
- **single points of failure**

The Gap Analysis basically compares your organization’s “As-Is” state with the Best Practice Incident Management process model. You can also compare your “As-Is” state to any other model. Through the comparison, you can identify areas for change and improvement.

You can also do a gap analysis without a comparison, simply by looking at your “As-Is and determining where you see

- 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



CERT Training and Education

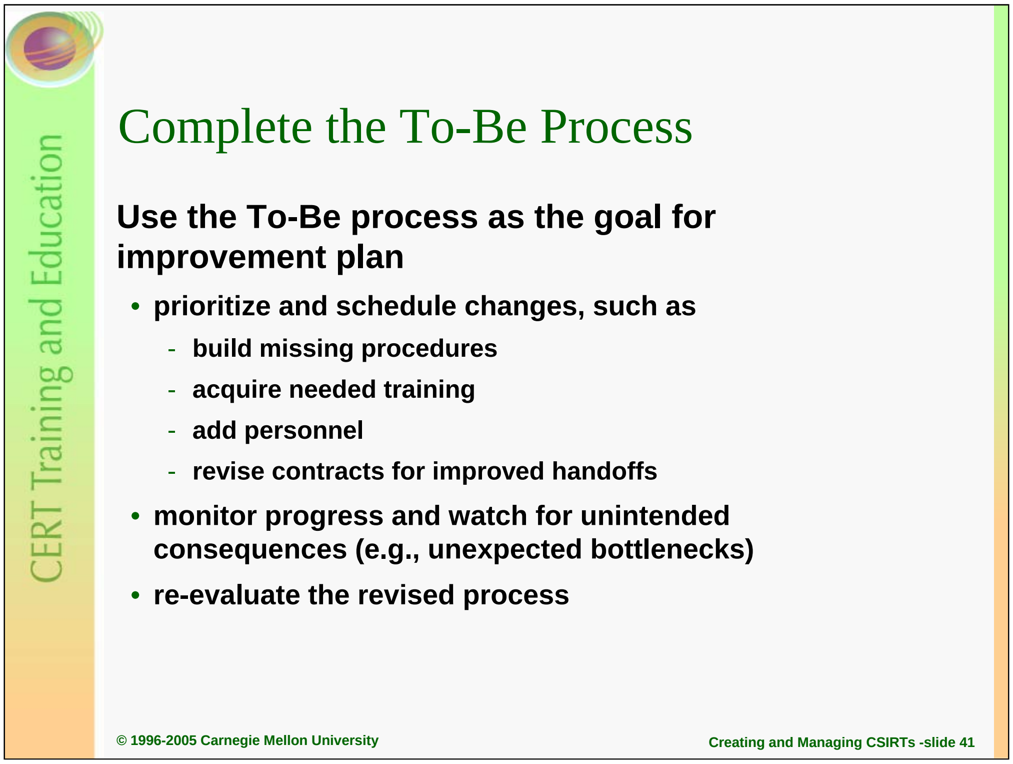
## Building the To-Be

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

- **identify new activities**
- **identify improvements to poor characteristics such missing procedures or poorly trained staff**
- **streamline inefficient flows**
- **redesign bottlenecks**

Creating and Managing CSIRTs -slide 40

In building the “To-Be” state, the desired process flows are designed. This is basically a mapping out of how you want to change the current process.



CERT Training and Education

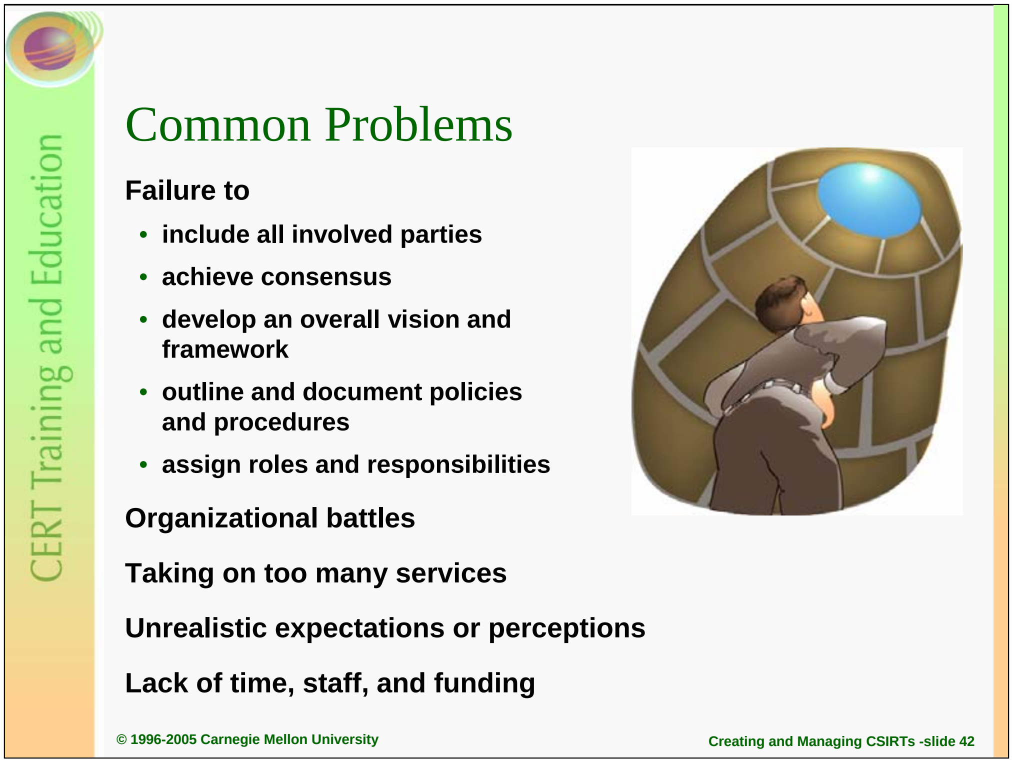
## Complete the To-Be Process

**Use the To-Be process as the goal for improvement plan**

- **prioritize and schedule changes, such as**
  - **build missing procedures**
  - **acquire needed training**
  - **add personnel**
  - **revise contracts for improved handoffs**
- **monitor progress and watch for unintended consequences (e.g., unexpected bottlenecks)**
- **re-evaluate the revised process**

Creating and Managing CSIRTs -slide 41

The “To-Be” process can be used as the basis for your process improvement plan. The process improvement plan details what changes you will make according to a devised schedule.


CERT Training and Education

## Common Problems

**Failure to**

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

**Organizational battles**

**Taking on too many services**

**Unrealistic expectations or perceptions**

**Lack of time, staff, and funding**

Creating and Managing CSIRTs -slide 42

Constraints can include

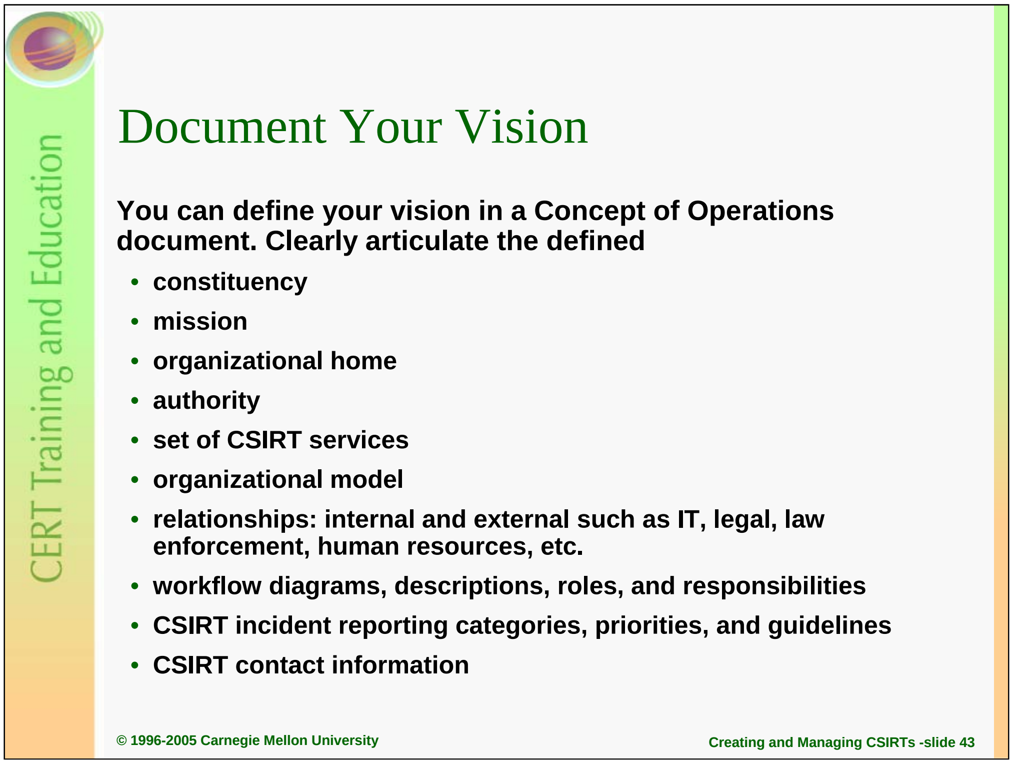
- budgets ceilings or lack of funding
- geographic dispersion of organization
- organizational disagreements or factions
- lack of management understanding and buy-in
- lack of experienced personnel resources
- lack of a clear vision, consensus, or expectation across the organization
- lack of communication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

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

- making sure everyone has a clear vision of what is happening
- making sure 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
- making sure 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 using more existing staff or extended staff
- collaborating with other CSIRTs  or other parts of your own organization to use parts of their services and expertise



CERT Training and Education

## Document Your Vision

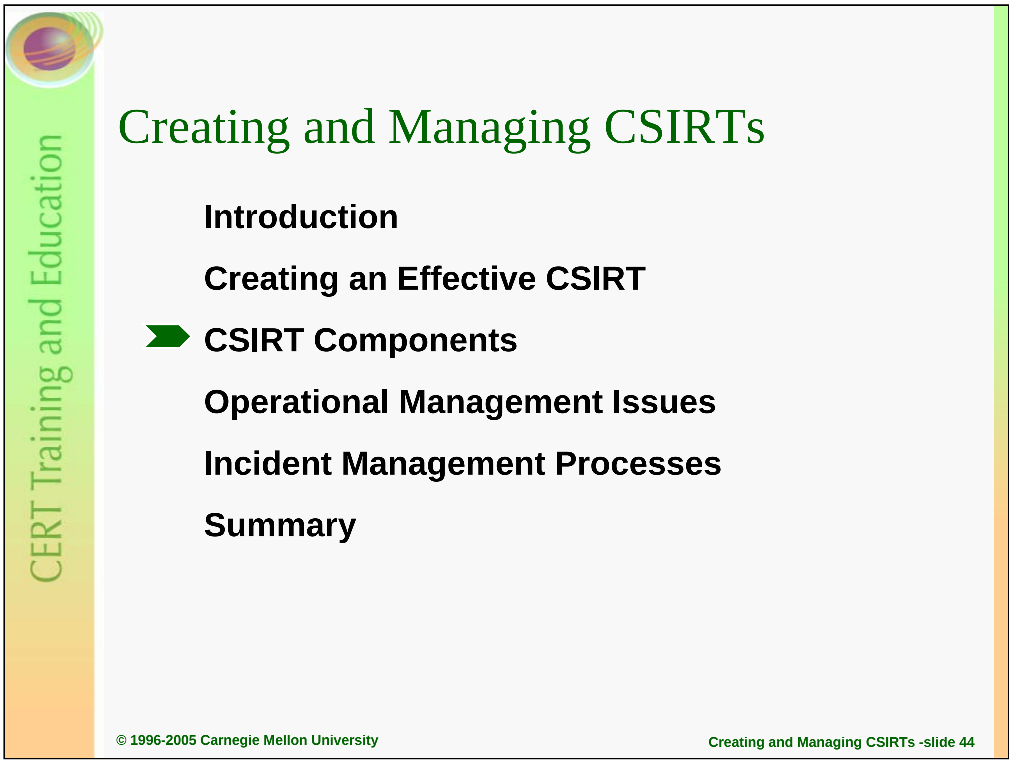
**You can define your vision in a Concept of Operations document. Clearly articulate the defined**

- **constituency**
- **mission**
- **organizational home**
- **authority**
- **set of CSIRT services**
- **organizational model**
- **relationships: internal and external such as IT, legal, law enforcement, human resources, etc.**
- **workflow diagrams, descriptions, roles, and responsibilities**
- **CSIRT incident reporting categories, priorities, and guidelines**
- **CSIRT contact information**

Creating and Managing CSIRTs -slide 43

You can outline your vision in a Concept of Operations document, defining each component and the interaction between the components and your host organization.

The next few slides will discuss defining the core CSIRT components.



CERT Training and Education

## Creating and Managing CSIRTs

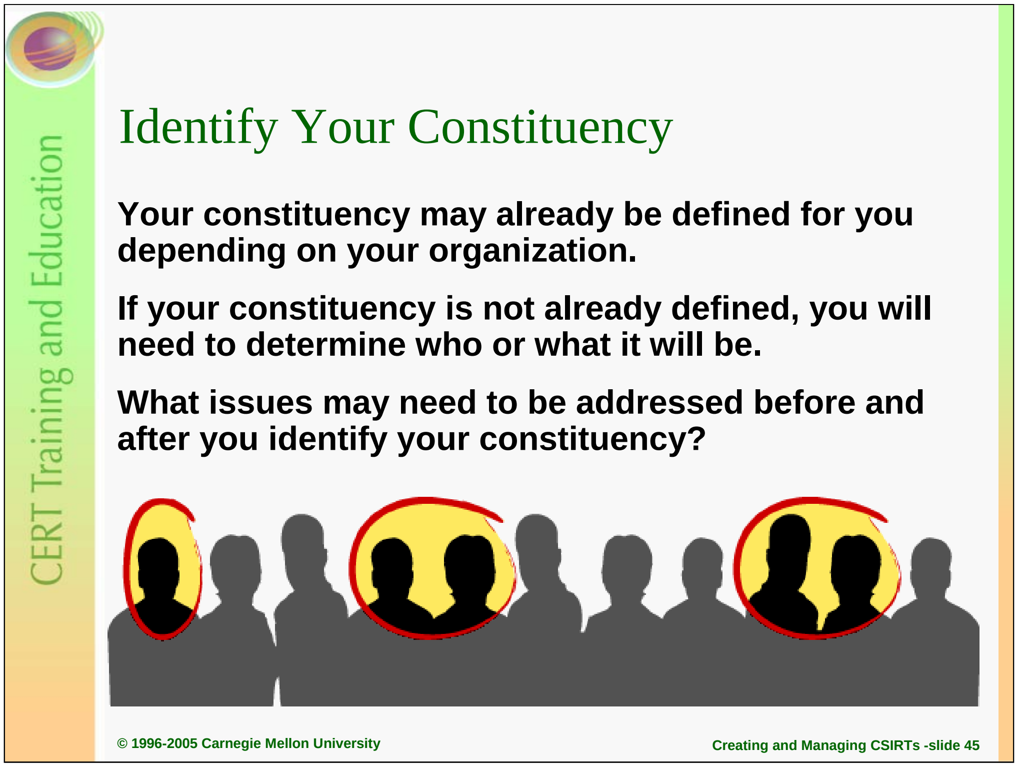
- Introduction
- Creating an Effective CSIRT
- ➤ CSIRT Components
- Operational Management Issues
- Incident Management Processes
- Summary

Creating and Managing CSIRTs -slide 44

The CSIRT Components include

- Constituency
- Mission
- Organizational Issues
- Funding
- Services
- Policies and Procedures
- Resources (discussed in next section)

Resources which are staffing, equipment, and infrastructure is discussed in the Operational Management Issues section of this presentation.



CERT Training and Education

## Identify Your Constituency

**Your constituency may already be defined for you depending on your organization.**

**If your constituency is not already defined, you will need to determine who or what it will be.**

**What issues may need to be addressed before and after you identify your constituency?**

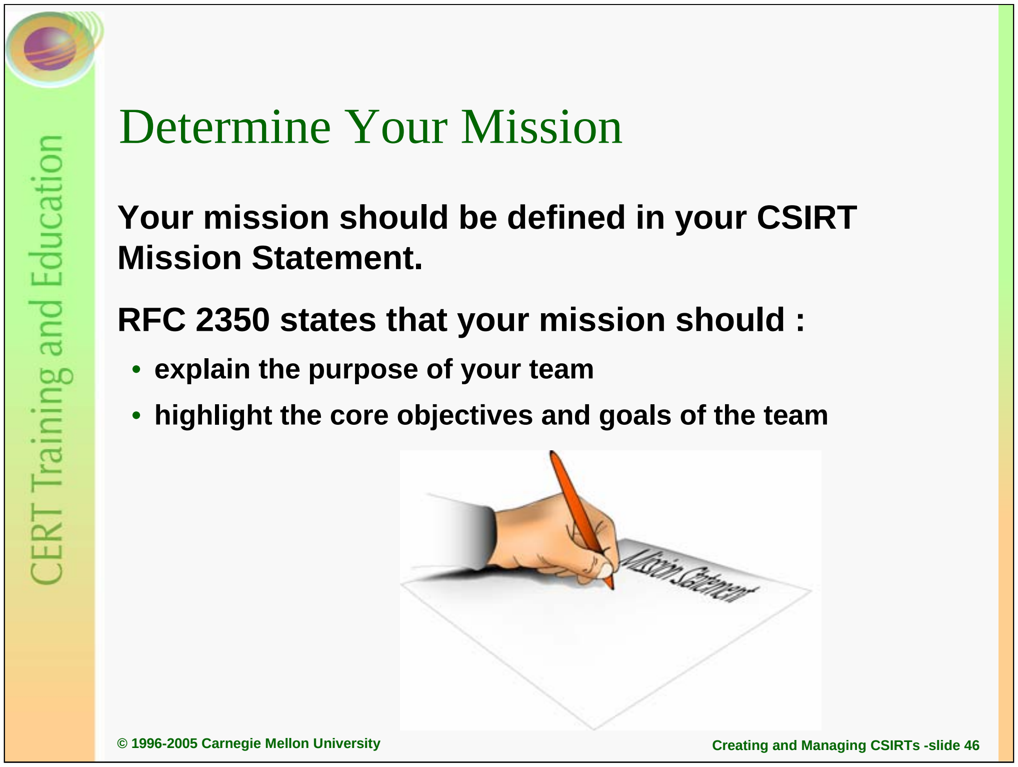
Creating and Managing CSIRTs -slide 45

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.

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.



CERT Training and Education

## Determine Your Mission

**Your mission should be defined in your CSIRT Mission Statement.**

**RFC 2350 states that your mission should :**

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

Mission Statement

© 1996-2005 Carnegie Mellon University

Creating and Managing CSIRTs -slide 46

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]

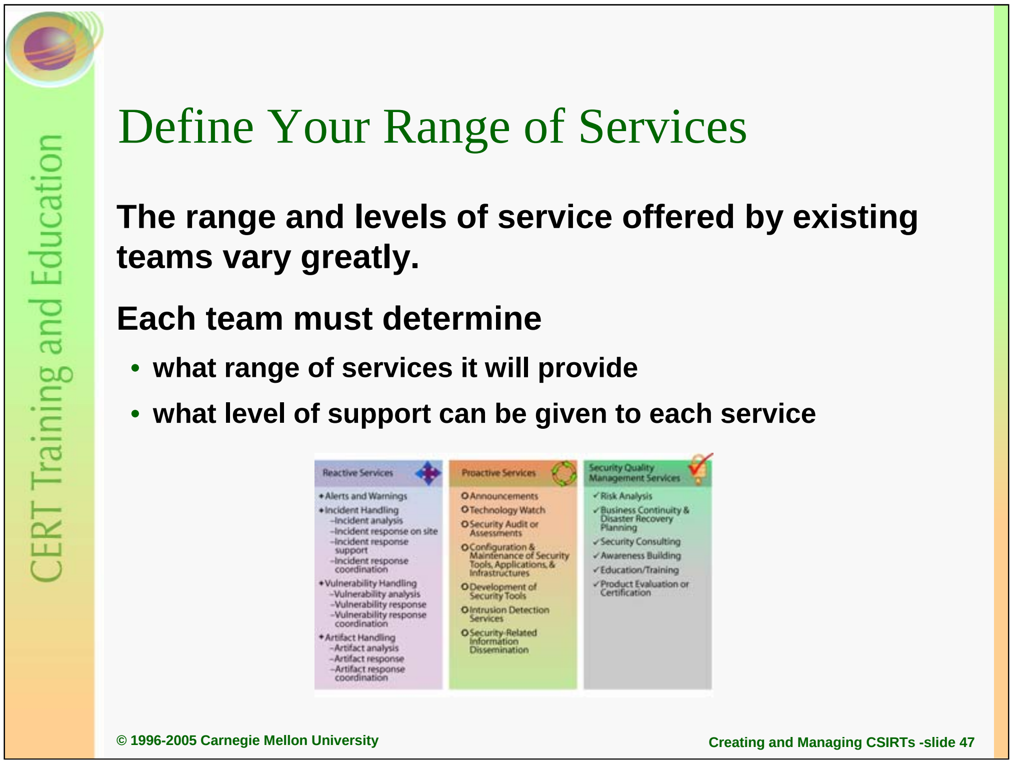
According to the CSIRT Handbook (page 8-9) your mission statement should:

- “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?

.



CERT Training and Education

## Define Your Range of Services

**The range and levels of service offered by existing teams vary greatly.**

**Each team must determine**

- **what range of services it will provide**
- **what level of support can be given to each service**

Reactive 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

Proactive Services

- ○ 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

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Creating and Managing CSIRTs -slide 47

Services selected should

- support the team mission
- reflect the resources available to support the service
- reflect the level of technical expertise available to the team

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 Federal Computer Incident Response Center (FedCIRC) or the CERT® Coordination Center (CERT/CC).

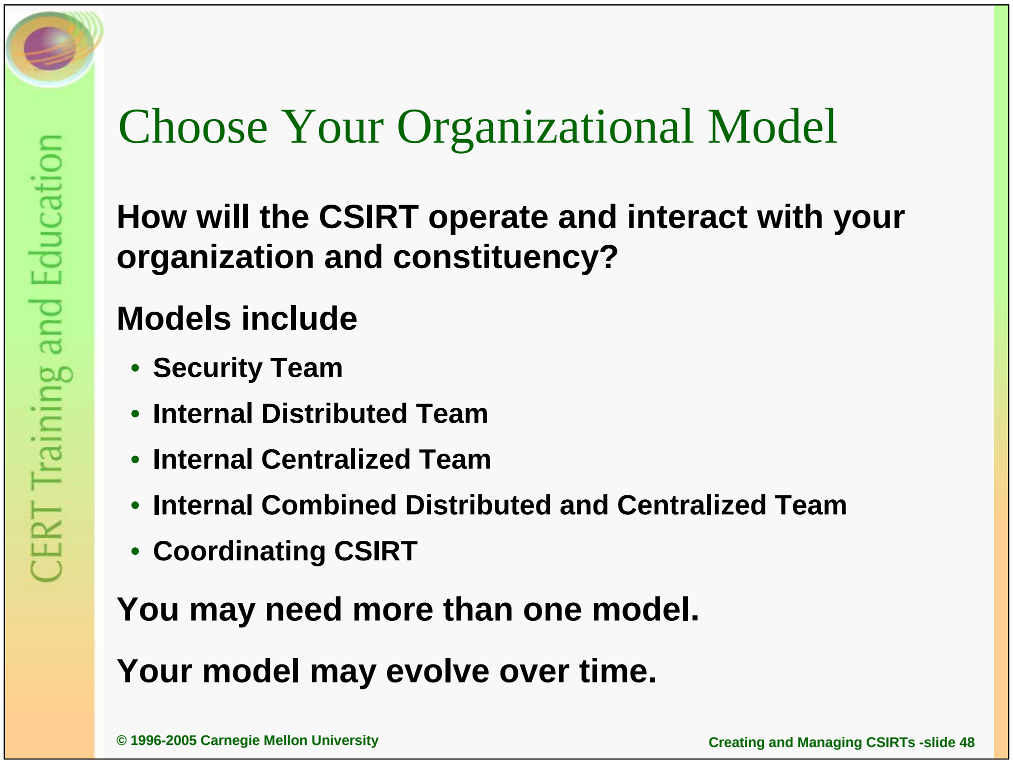
It is recommended that a CSIRT start with a small subset of services, gain acceptance of the CSIRT by the organization through quality service and response, then begin to develop and expand the capabilities of the CSIRT as they are needed and can be effectively supported.

All services offered should be defined to clearly set the expectations of all internal and external parties involved.

Remember, no single team can be everything to everyone!

For every service your CSIRT offers, you need to clearly define

- the depth and breadth at which that service is provided
- how many resources are assigned to the service
- what level of expertise is required to provide the service?
- what requirements or criteria must be met?
  - service level agreements (SLAs)
  - federal or state regulations
  - response timeframes



CERT Training and Education

## Choose Your Organizational Model

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

**Models include**

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

**You may need more than one model.**

**Your model may evolve over time.**

Creating and Managing CSIRTs -slide 48

Here are some sample organizational models. Each type of CSIRT Model has its strengths, weaknesses, and benefits. 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

Model definitions – For more in depth discussion please see: http://www.cert.org/archive/pdf/03hb001.pdf

**Security Team -** In this model, no group or section of the organization has been given the formal responsibility for all incident handling activities. No CSIRT has been established.

**Internal Distributed Team** – In this model, the organization utilizes existing staff to provide a “virtual” distributed CSIRT, which is formally chartered to deal with incident response activities.

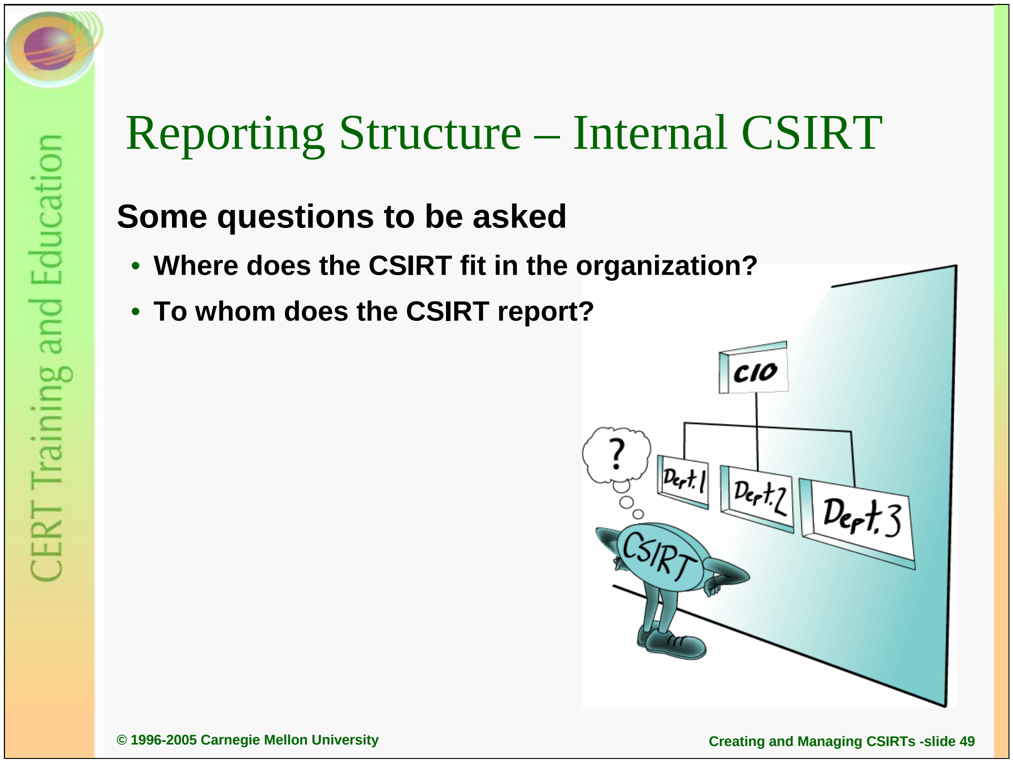
**Internal Centralized Team** – This model is a fully staffed, dedicated CSIRT that provides the incident handling services for a defined constituency, 100% of the time.

**Internal Combined Distributed and Centralized Team** – This model represents a combination of the distributed CSIRT and the centralized CSIRT.

**Coordinating CSIRT** – In this model the CSIRT coordinates and facilitates the handling of incidents across a variety of external organizations.

You may need more than one model. For example, consider a large, geographically dispersed organization. It might require local teams on site, reporting to a regional, centralized CSIRT with each regional CSIRT then reporting to a Coordination Center who then passes synthesized information to an Analysis Team for further research on trends and patterns.

One important thing to remember is that you cannot always do everything at once. You may need to incrementally add resources. Many teams start out only providing Incident Handling services and grow into other services and other models as resources, budgets, and support allow. Your model may need to be revised over time based on changes in your mission, priorities, provided services, or sponsorship.



CERT Training and Education

# Reporting Structure – Internal CSIRT

**Some questions to be asked**

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

Creating and Managing CSIRTs -slide 49

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.

A CSIRT could be located in the IT or telecommunications department, the security group, or be its own unit. The CSIRT could report to the CIO, the CEO, the CSO, or another department head.

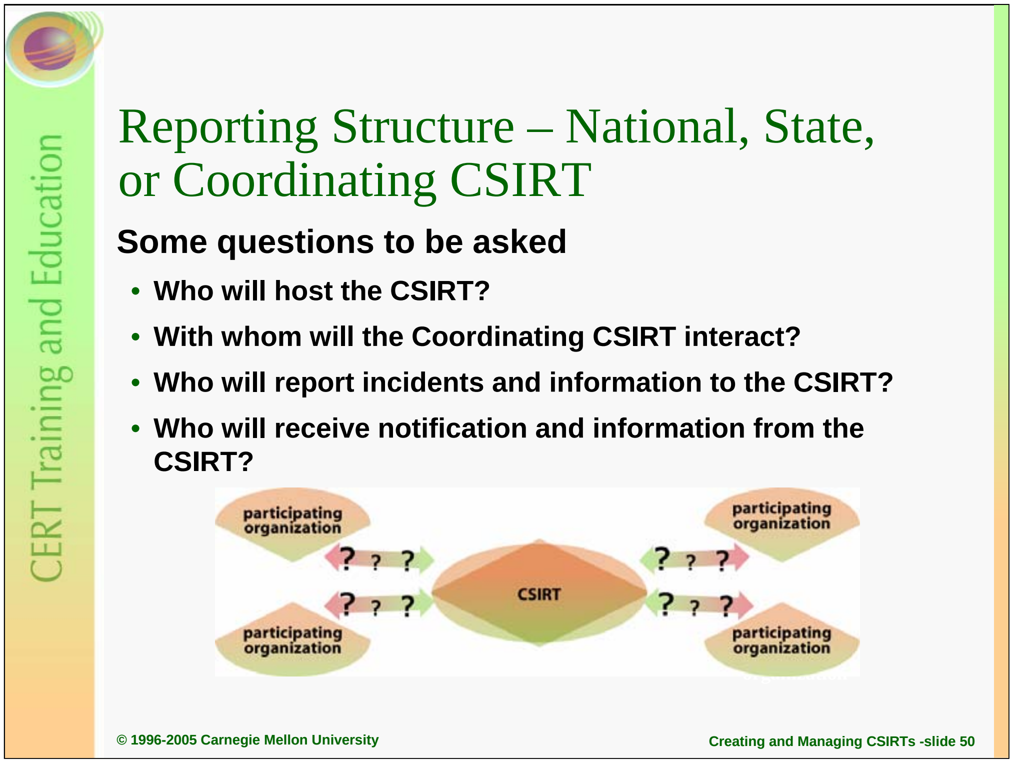
It is important to think about what actions the CSIRT will need to take and what type of management support will be required to facilitate those actions during incident handling and response. Identifying such issues may suggest the right reporting or management structure.

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.

The definition of the CSIRT authority goes hand-in-hand with the first two bullets listed above. How much authority the CSIRT will have to make decisions about incident response, recovery and security prevention will be impacted by where and to whom the CSIRT reports in the organizational structure.

Questions to ask include:

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



CERT Training and Education

## Reporting Structure – National, State, or Coordinating CSIRT

**Some questions to be asked**

- **Who will host the CSIRT?**
- **With whom will the Coordinating CSIRT interact?**
- **Who will report incidents and information to the CSIRT?**
- **Who will receive notification and information from the CSIRT?**

participating organization
participating organization
? ? ?
? ? ?
CSIRT
? ? ?
? ? ?
participating organization
participating organization

Creating and Managing CSIRTs -slide 50

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

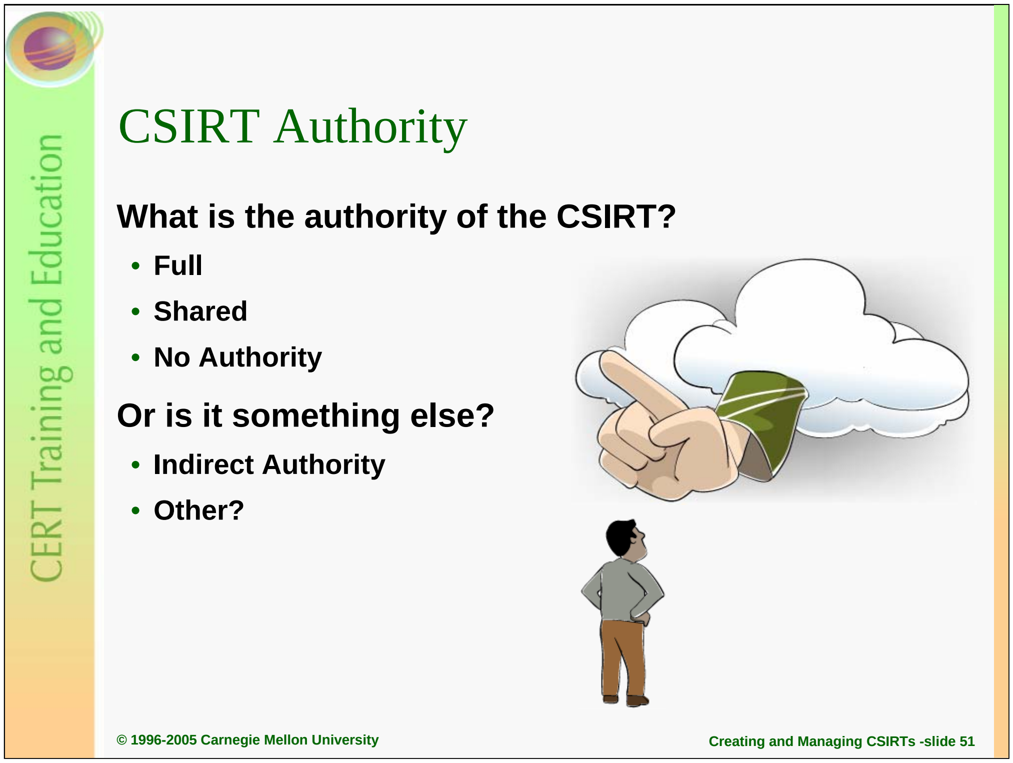
- Government organizations
- Military organizations
- Critical infrastructures
- Business organizations

Or will the CSIRT accept reports from and disseminate information to the public.

Some questions to ask include:

- What information will the CSIRT provide to the constituency?
- What information will the constituency provide to the CSIRT?
- How will the Coordinating CSIRT interact with the existing constituency CSIRTs?

Some issues to think about is to whom and in what time frame will the Coordinating CSIRT pass out advisories and alerts? Many constituent CSIRTs may have already received this information from other sources.



CERT Training and Education

## CSIRT Authority

**What is the authority of the CSIRT?**

- **Full**
- **Shared**
- **No Authority**

**Or is it something else?**

- **Indirect Authority**
- **Other?**

Creating and Managing CSIRTs -slide 51

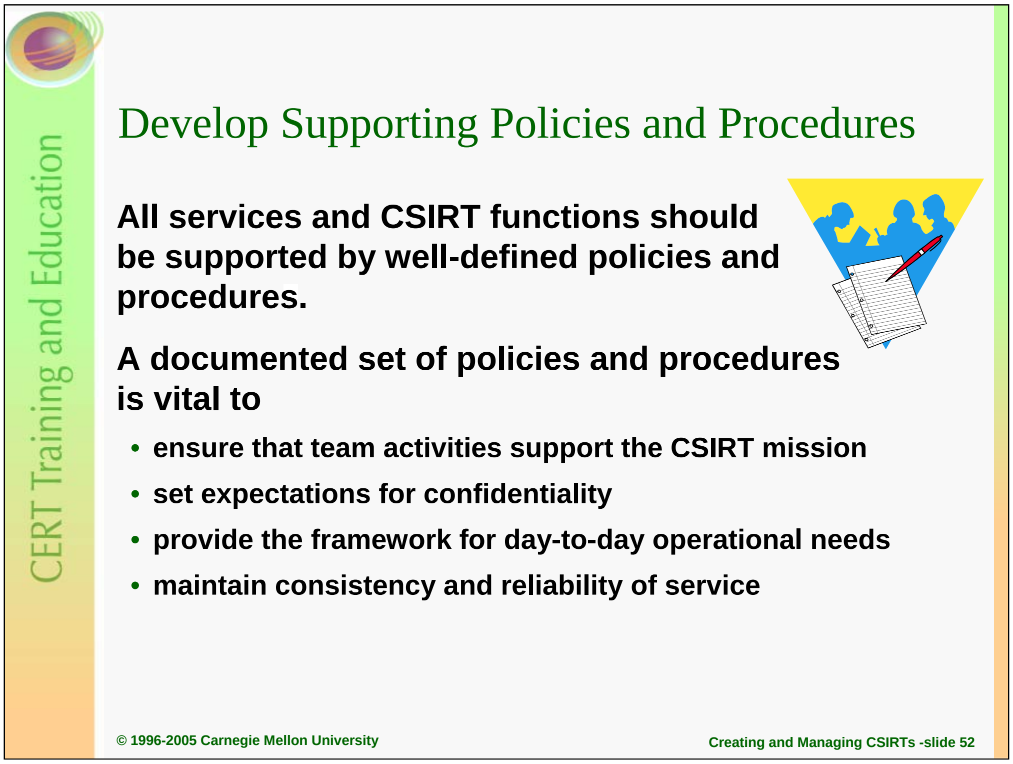
Authority describes the control that the CSIRT has over its own actions and the actions of its constituents, related to computer security and incident response. Authority is the basic relationship the CSIRT has to the organization it serves.

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.



CERT Training and Education

## Develop Supporting Policies and Procedures

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

**A documented set of policies and procedures is vital to**

- **ensure that 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**

Creating and Managing CSIRTs -slide 52

Documented policies and procedures are vital to the success of your CSIRT.

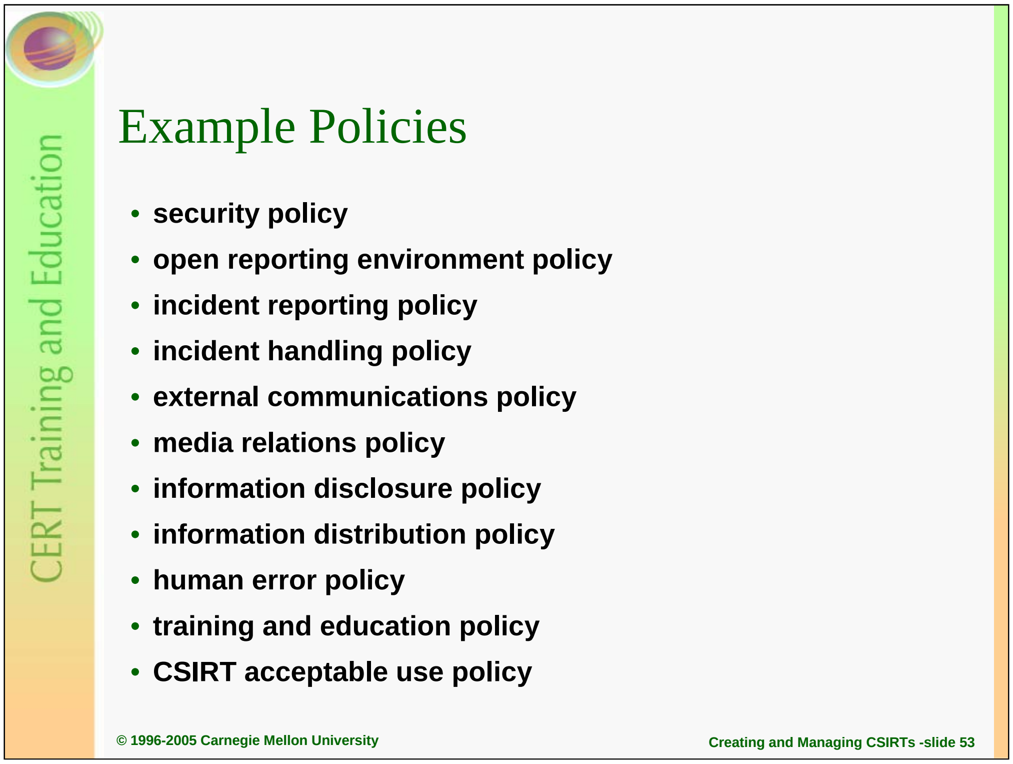
Well-defined policies and procedures offer guidance for CSIRT staff operations.

Once services are chosen you must build or document operations through CSIRT policies and procedures. Well-defined policies and procedures offer guidance for

- roles and responsibilities
- priorities
- escalation criteria
- the nature of responses given
- new CSIRT staff members

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.



CERT Training and Education

## Example Policies

- 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
- CSIRT acceptable use policy

Creating and Managing CSIRTs -slide 53

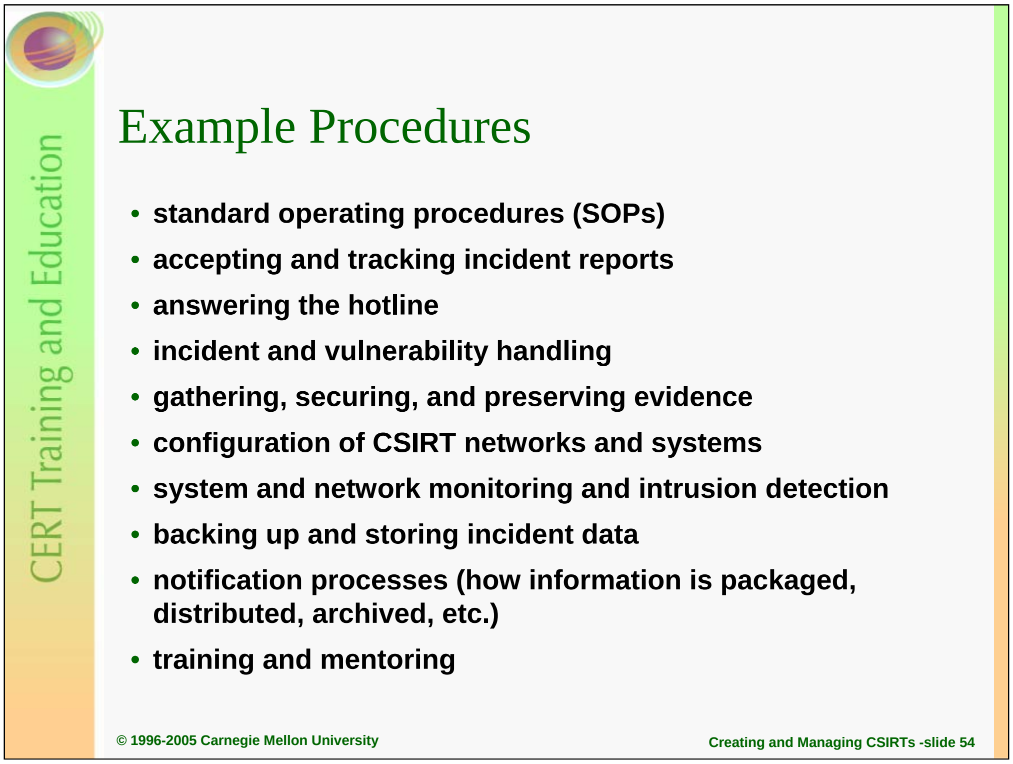
Policies must be clearly understood so that staff can correctly implement procedures and enact their responsibilities.

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.



CERT Training and Education

## Example Procedures

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

Creating and Managing CSIRTs -slide 54

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.

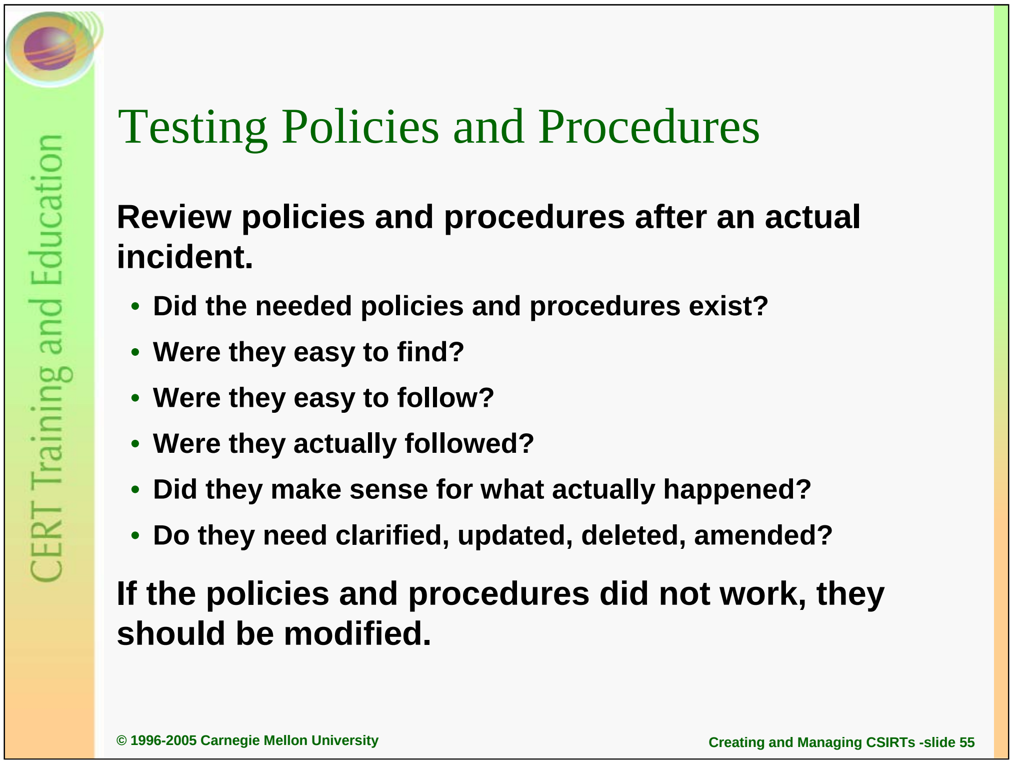
Along with creating organizational procedures management must also decide who will create the procedures and where they will reside.

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.

Take a few minutes and think about the types procedures your CSIRT might need.


CERT Training and Education

## Testing Policies and Procedures

**Review policies and procedures after an actual incident.**

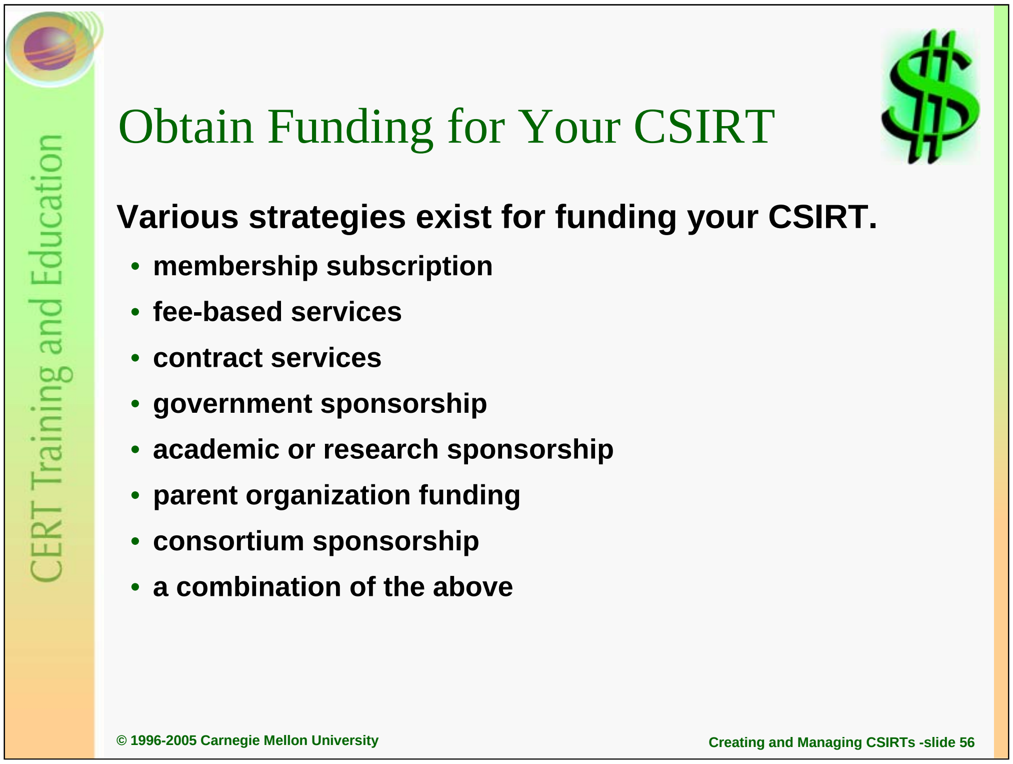
- **Did the needed policies and procedures exist?**
- **Were they easy to find?**
- **Were they easy to follow?**
- **Were they actually followed?**
- **Did they make sense for what actually happened?**
- **Do they need clarified, updated, deleted, amended?**

**If the policies and procedures did not work, they should be modified.**

Creating and Managing CSIRTs -slide 55

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.



## 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

- ad hoc payment for services as delivered
- CanCERT and MYCERT had fee-based services.

Contract services

- outsource CSIRT to organization providing incident handling service
- commercial groups such as IBM, CISCO, many top consulting firms

Government sponsorship

- government funds the CSIRT
- FedCIRC is sponsored by the U.S. government.

Academic or research sponsorship

- university or research network funds the CSIRT
- DANTE, NORDUnet are both sponsored by research networks.

Parent organization funding

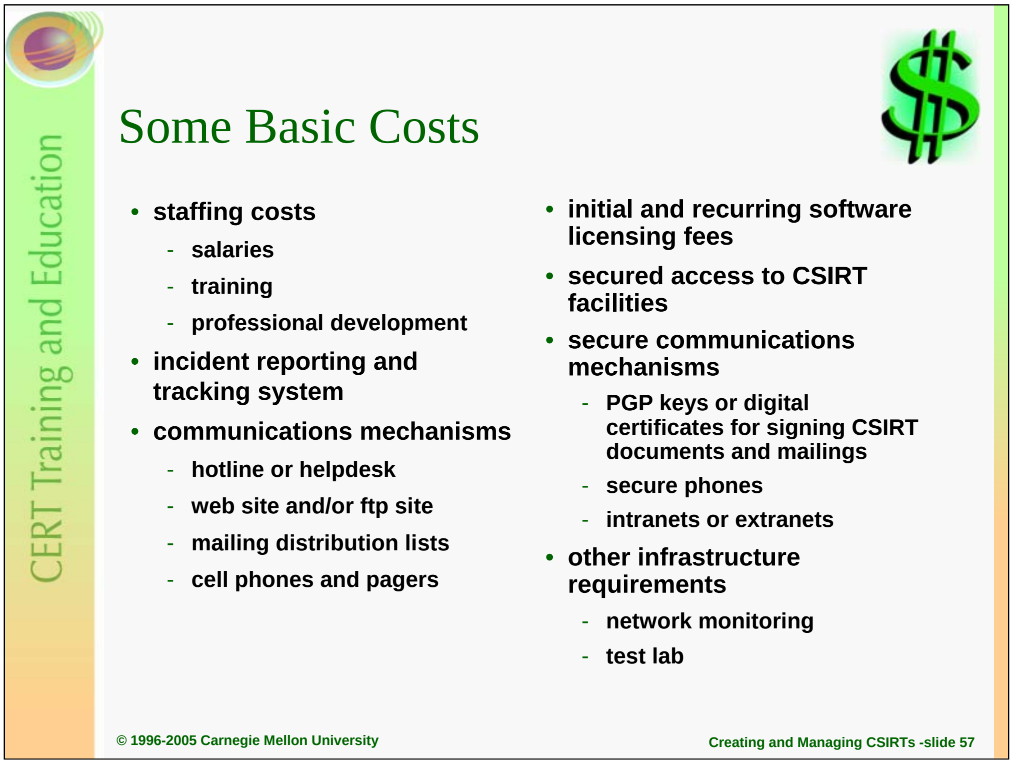
- parent organization establishes and funds CSIRT
- IBM, GE, and Compaq CSIRTs are members of FIRST.

Consortium sponsorship

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

Combination of the above

- CERT/CC is funded by government and private sponsorship.



CERT Training and Education

## Some Basic Costs

- staffing costs
  - salaries
  - training
  - professional development
- incident reporting and tracking system
- communications mechanisms
  - hotline or helpdesk
  - web site and/or ftp site
  - mailing distribution lists
  - cell phones and pagers
- initial and recurring software licensing fees
- secured access to CSIRT facilities
- secure communications mechanisms
  - PGP keys or digital certificates for signing CSIRT documents and mailings
  - secure phones
  - intranets or extranets
- other infrastructure requirements
  - network monitoring
  - test lab

Creating and Managing CSIRTs -slide 57

We will discuss these in more depth in later sections.

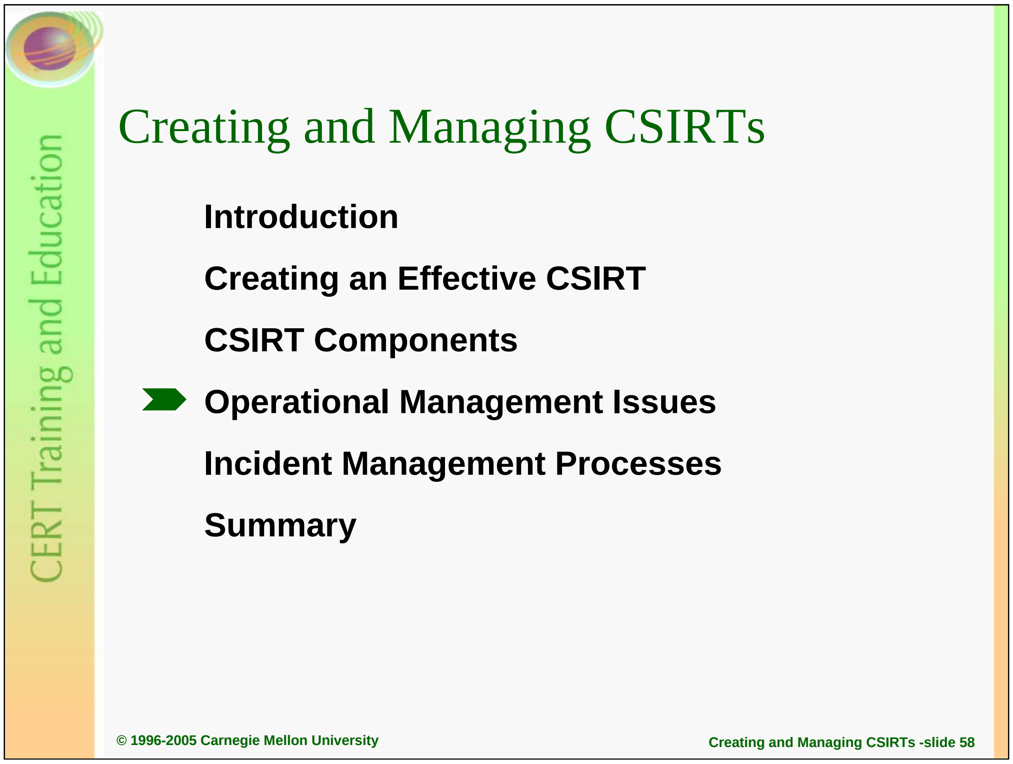
Once you have an idea of your services and the resources you need to provide to support those services, you will need to plan a budget to be presented for short-term and long-term funding.

Where will you obtain this funding?

Some resources for helping to establish the cost of an incident

- Incident Cost and Analysis Model Project
  http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml
- Computer Crime and Security Survey
  from Computer Security Institute (CSI) in partnership with the FBI
  http://www.gocsi.com/press/20030528.jhtml
  http://www.gocsi.com/forms/fbi/pdf.jhtml

You may be able to establish what an incident might cost you, and then use that in a cost/benefit analysis to show the amount of money a CSIRT might save your organization.



CERT Training and Education

# Creating and Managing CSIRTs

Introduction

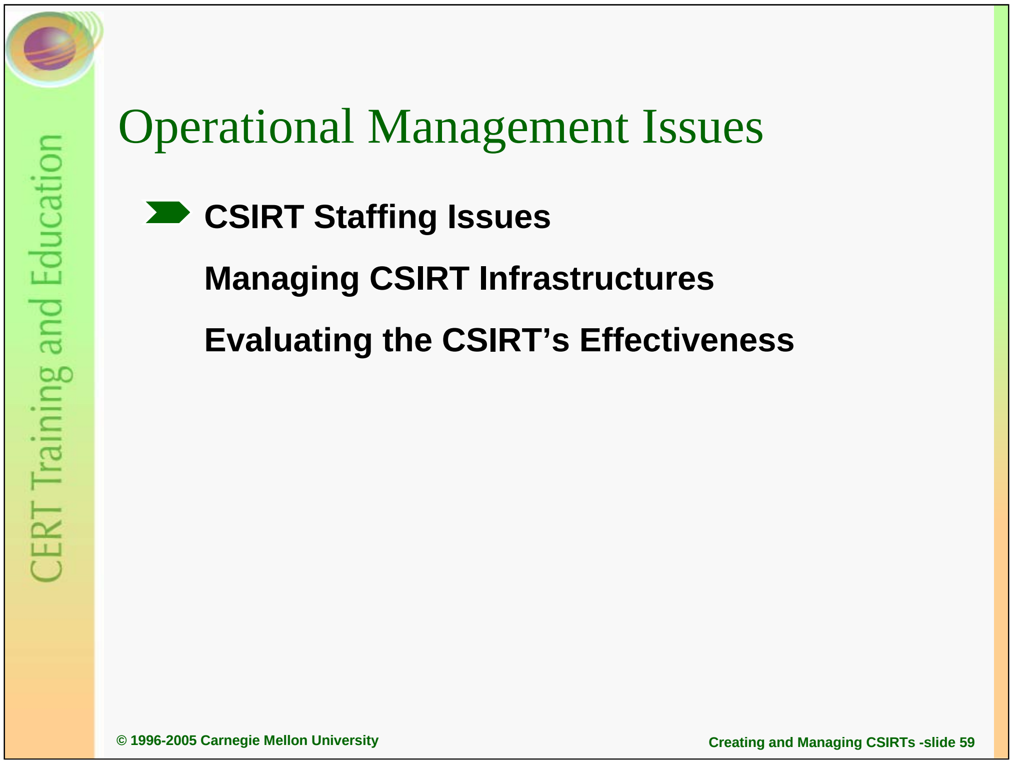
Creating an Effective CSIRT

CSIRT Components

➤ Operational Management Issues

Incident Management Processes

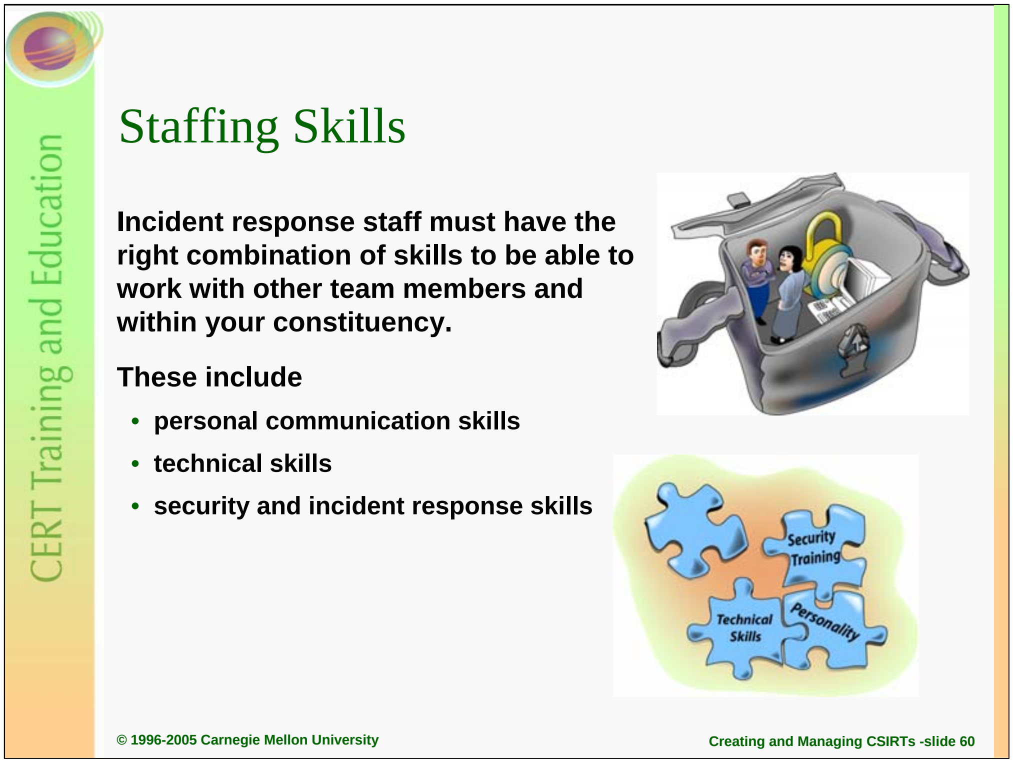
Summary



CERT Training and Education

# Operational Management Issues

- **CSIRT Staffing Issues**
- **Managing CSIRT Infrastructures**
- **Evaluating the CSIRT’s Effectiveness**


CERT Training and Education
Security Training
Technical Skills
Personality

## Staffing Skills

**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**

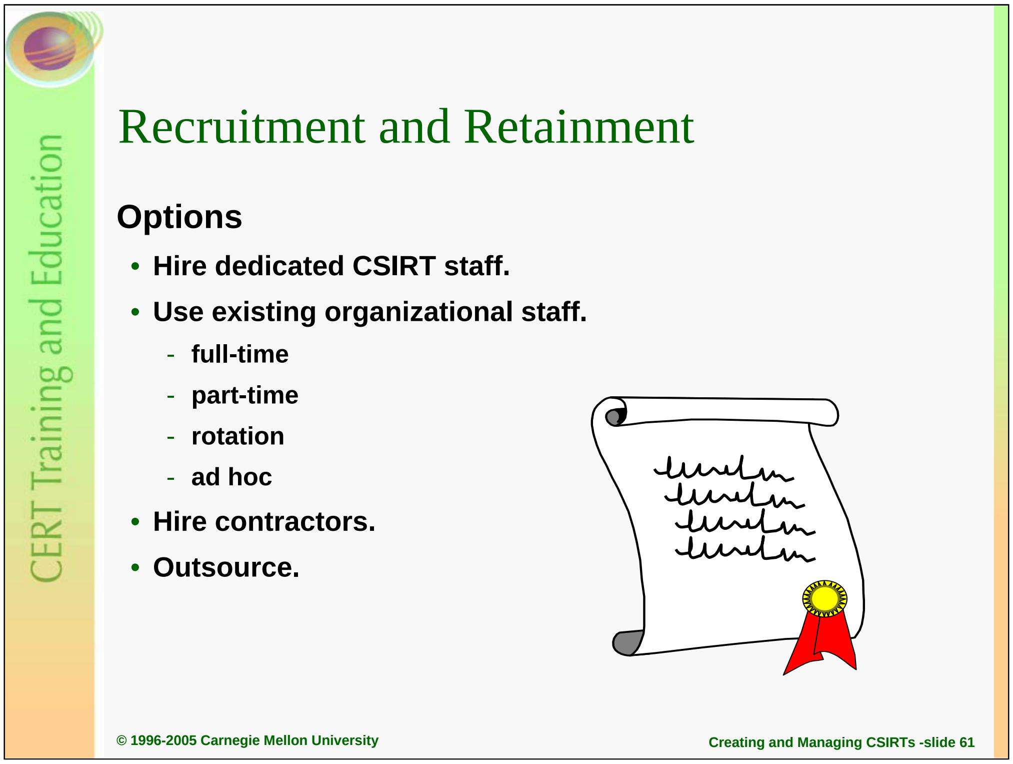
Creating and Managing CSIRTs -slide 60

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, NT, Windows, Linux, Macintosh
  - basic understanding of Internet protocols
  - Basic understanding of common computer attacks and vulnerabilities
- Security Training
  - incident handling experience
  - problem solving abilities



CERT Training and Education

## Recruitment and Retainment

**Options**

- **Hire dedicated CSIRT staff.**
- **Use existing organizational staff.**
  - **full-time**
  - **part-time**
  - **rotation**
  - **ad hoc**
- **Hire contractors.**
- **Outsource.**

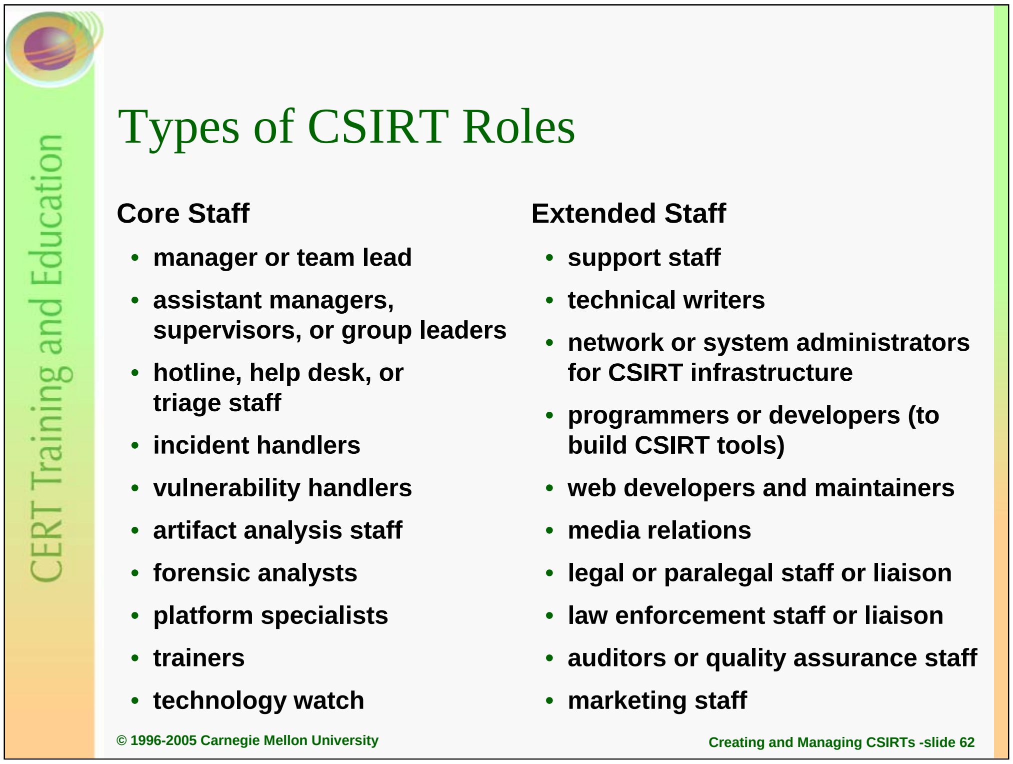
Creating and Managing CSIRTs -slide 61

Hiring or obtaining the right staff is critical to the success of your CSIRT team. Incident response staff must have the right type of personal communication skills to be able to work with other team members and within your constituency. They must be able to deal with the slow days and the hectic days.

When creating a CSIRT, one of the most important questions you must answer will concern where and how you will obtain your staff.

- 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 needed information.
- 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.

The biggest problem across all options is that there are not enough experienced incident handlers to fill all the open positions. To counter that, some universities are beginning to offer programs in information assurance and cyber security.



CERT Training and Education

## Types of CSIRT Roles

**Core Staff**

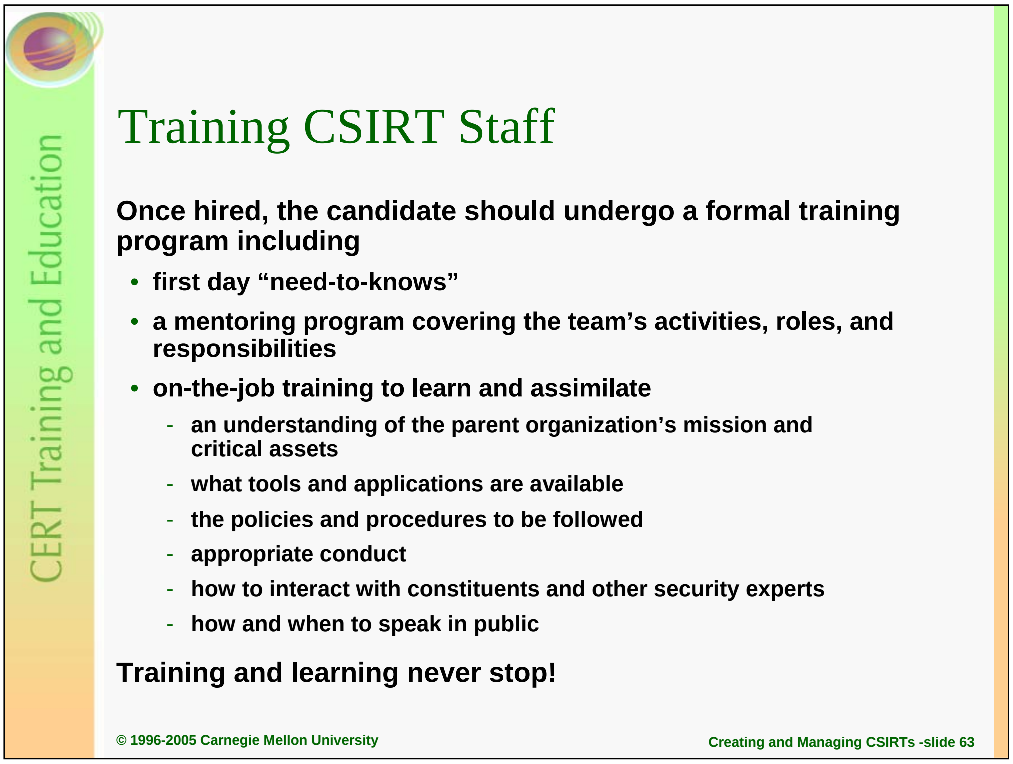
- manager or team lead
- assistant managers, supervisors, or group leaders
- hotline, help desk, or triage staff
- incident handlers
- vulnerability handlers
- artifact analysis staff
- forensic analysts
- platform specialists
- trainers
- technology watch

**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.



CERT Training and Education

## Training CSIRT Staff

**Once hired, the candidate should undergo a formal training program including**

- **first day “need-to-knows”**
- **a mentoring program covering the team’s activities, roles, and responsibilities**
- **on-the-job training to learn and assimilate**
  - **an understanding of the parent organization’s mission and critical assets**
  - **what tools and applications are available**
  - **the policies and procedures to be followed**
  - **appropriate conduct**
  - **how to interact with constituents and other security experts**
  - **how and when to speak in public**

**Training and learning never stop!**

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

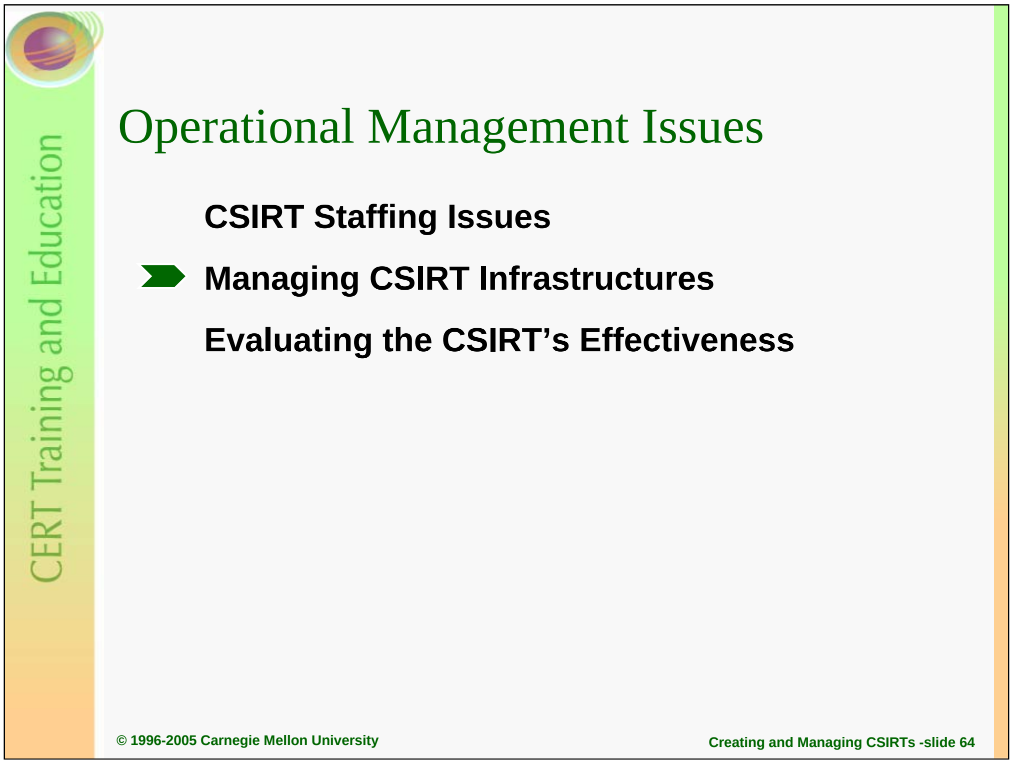
On the first day let the new CSIRT staff member know exactly what they can and can not say. It is important that they learn and understand your team’s information disclosure policy.

CERT/CC has a series of presentations and training that a new team member must attend, including

- confidentiality briefing
- CERT-speak – CERT/CC media policy
- CERT/CC Code of Conduct

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

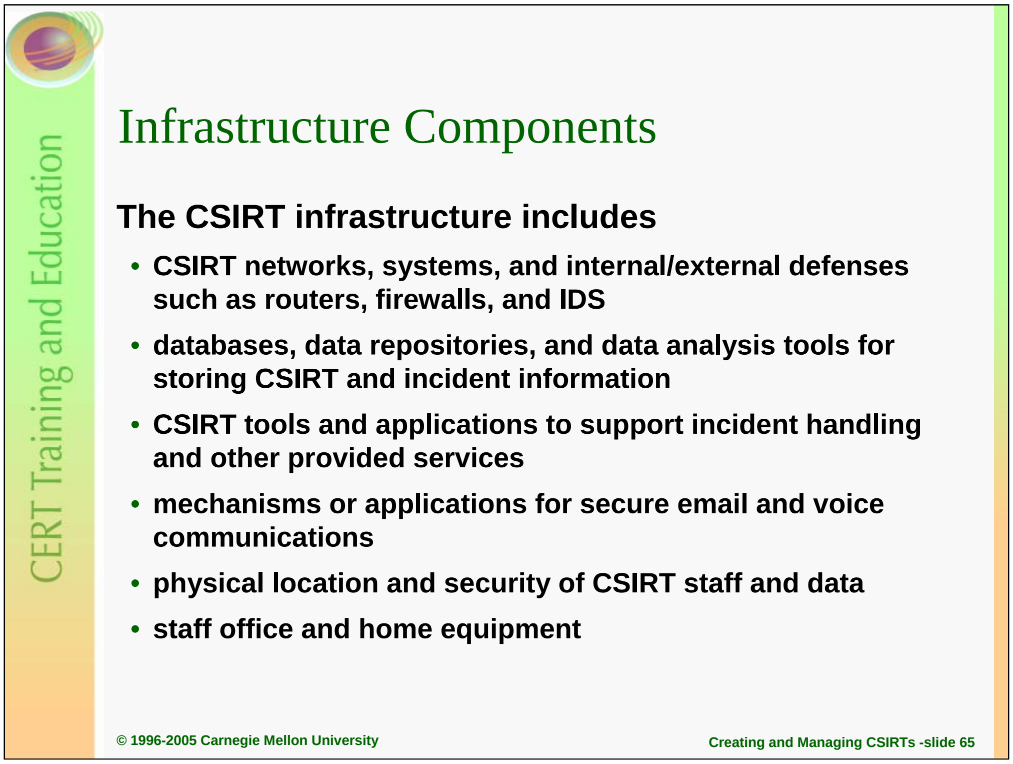
- CERT Managers, Technical Staff, and Incident Handler Courses
  http://www.cert.org/training/
- SANS GIAC Certification and Training Program
  http://www.giac.org/


CERT Training and Education

## Operational Management Issues

- CSIRT Staffing Issues
- ➤ Managing CSIRT Infrastructures
- Evaluating the CSIRT’s Effectiveness

Creating and Managing CSIRTs -slide 64



CERT Training and Education

# Infrastructure Components

**The CSIRT infrastructure includes**

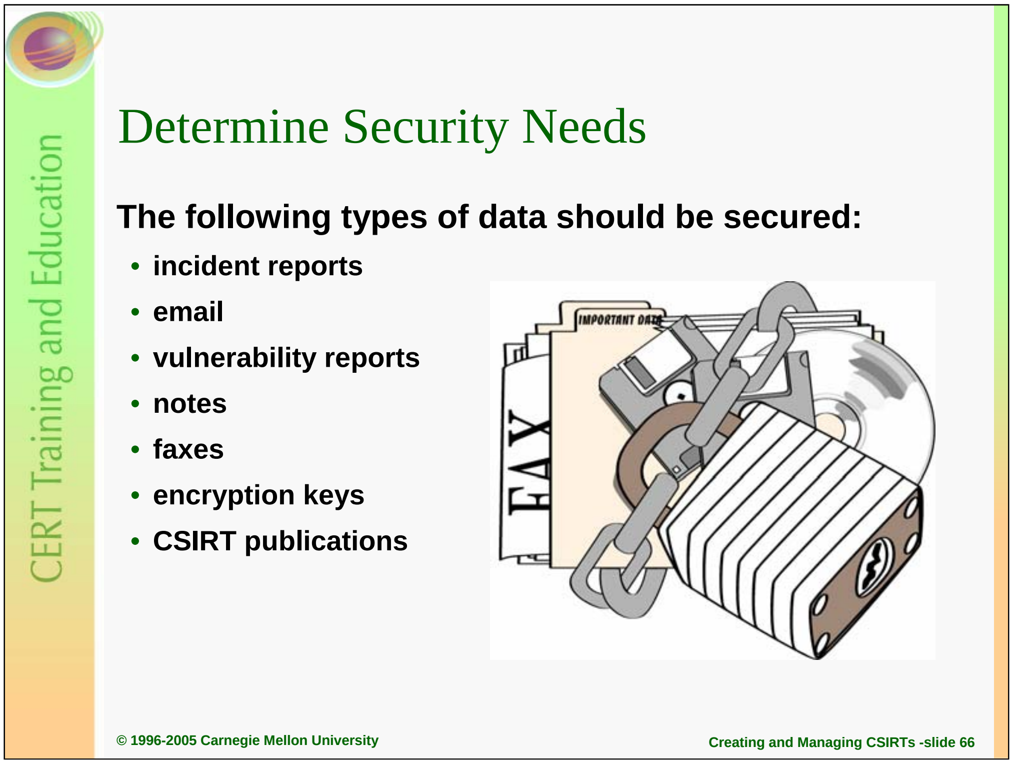
- **CSIRT networks, systems, and internal/external defenses such as routers, firewalls, and IDS**
- **databases, data repositories, and data analysis tools for storing CSIRT and incident information**
- **CSIRT tools and applications to support incident handling and other provided services**
- **mechanisms or applications for secure email and voice communications**
- **physical location and security of CSIRT staff and data**
- **staff office and home equipment**

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.

You may want to refer to OCTAVE, a self-directed method of risk evaluation that helps you identify and protect your critical assets.

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



CERT Training and Education

## Determine Security Needs

**The following types of data should be secured:**

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

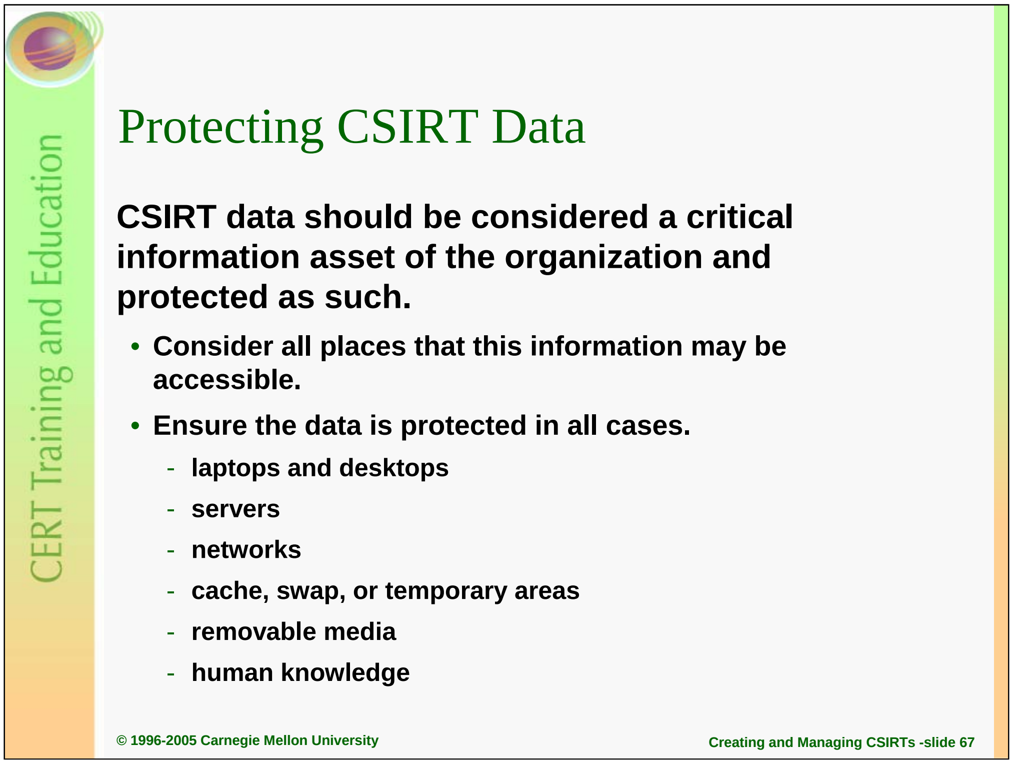
IMPORTANT DATA
FAX

© 1996-2005 Carnegie Mellon University

Creating and Managing CSIRTs -slide 66

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

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).



CERT Training and Education

## Protecting CSIRT Data

**CSIRT data should be considered a critical information asset of the organization and protected as such.**

- **Consider all places that this information may be accessible.**
- **Ensure the data is protected in all cases.**
  - **laptops and desktops**
  - **servers**
  - **networks**
  - **cache, swap, or temporary areas**
  - **removable media**
  - **human knowledge**

Creating and Managing CSIRTs -slide 67

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

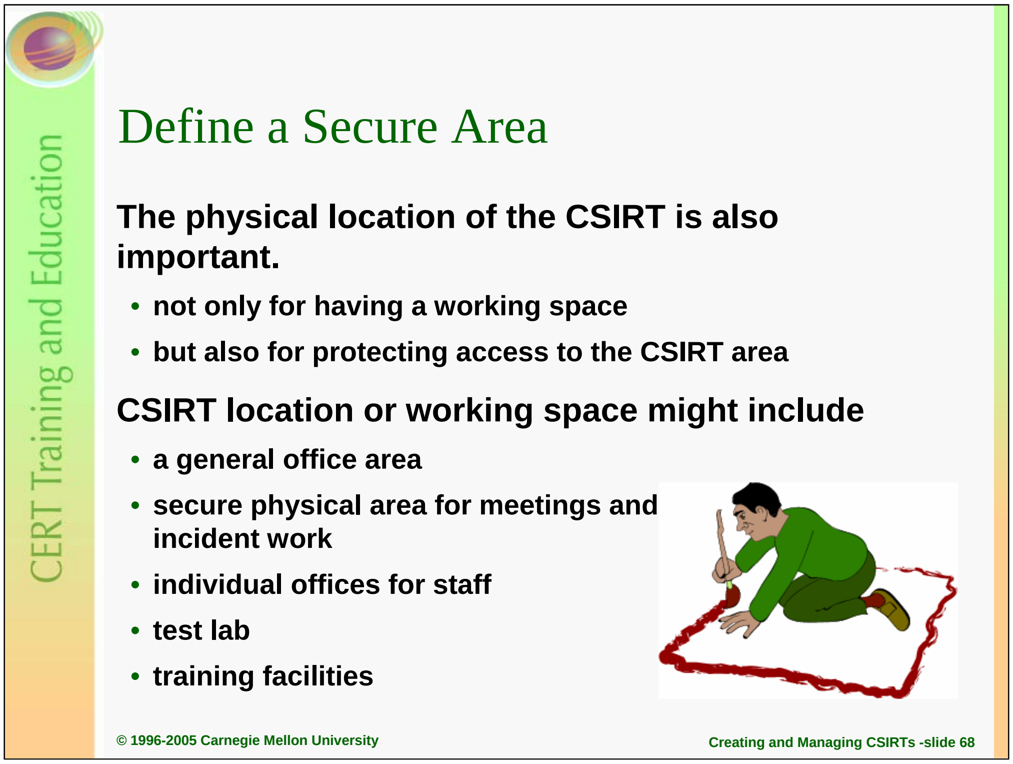
- legal requirements
- constituency expectations
- business necessity
- potential intruder threat

What you need to know to protect data

- Where is the data created/received?
- Where is the data stored?
- What path does the data travel from location to location?
- Who has access to the data?

Secure each location where data is stored and the path the data travels.

- Physically secure servers and workstations containing sensitive information.
- Erase electronic media containing sensitive information before reusing it.
- Erase or destroy electronic media before disposal.


CERT Training and Education

## Define a Secure Area

**The physical location of the 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**
- **individual offices for staff**
- **test lab**
- **training facilities**

© 1996-2005 Carnegie Mellon University

Creating and Managing CSIRTs -slide 68

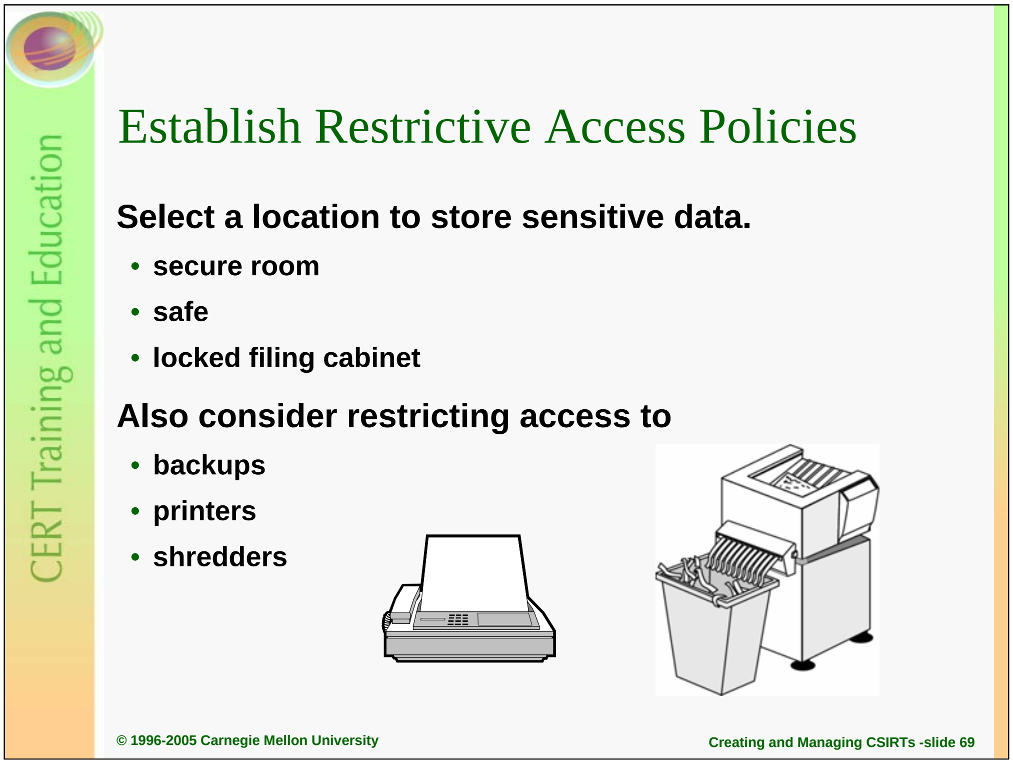
Is the data protected in case of natural disasters?

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



CERT Training and Education

## Establish Restrictive Access Policies

**Select a location to store sensitive data.**

- **secure room**
- **safe**
- **locked filing cabinet**

**Also consider restricting access to**

- **backups**
- **printers**
- **shredders**

Creating and Managing CSIRTs -slide 69

Select a location to store sensitive data.

- secure room
- safe
- locked filing cabinet

Determine who should have access to the data. Restrict access by unauthorized persons, including

- janitor/maintenance staff
- other employees not involved in incident handling

Backups

- Backups should be stored in a secure location.
- Backups should be encrypted.
- Backup media must be disposed of properly.
- In addition, offsite backups should be transported in a secure manner.

Printers

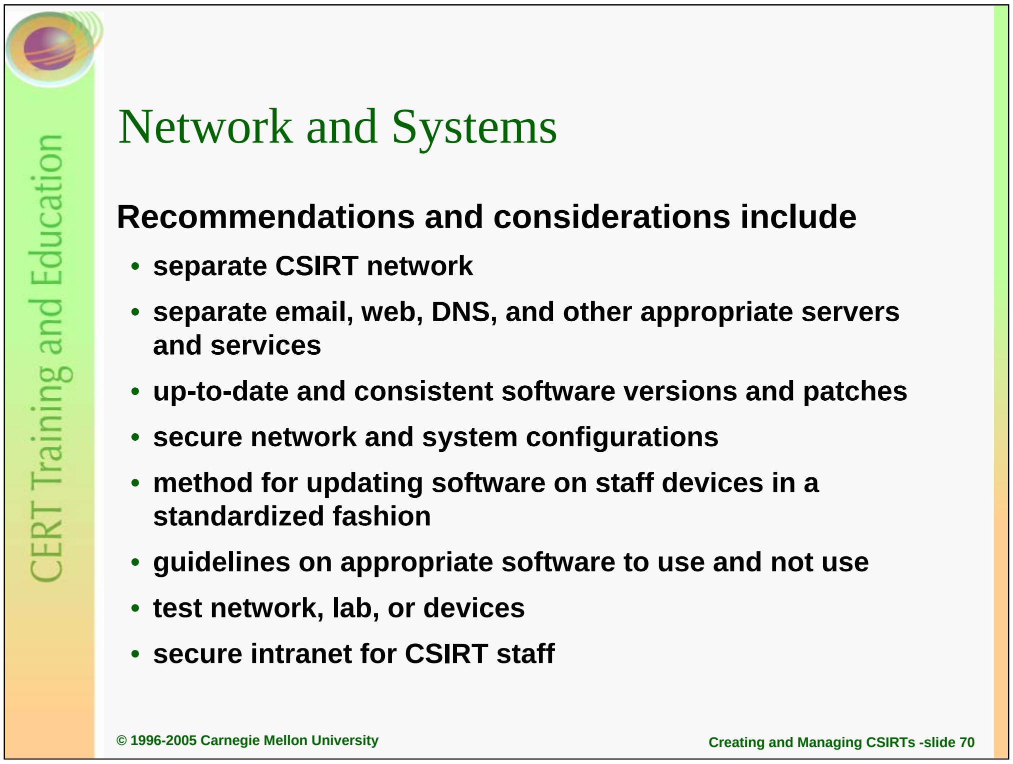
- Locate printers that are used to print sensitive data in a secure area.
- Store output from printers in a secure location.
- Remember: FAX machines are printers, too.

Shredders

- Store papers to be shredded in a secure location prior to shredding.
- Shredding should be performed by personnel authorized to see sensitive data.
- Shredding equipment should meet the standards set by the sensitivity of the materials to be shredded.

Servers which house CSIRT data including web, email, DNS, or application servers – should be located in a secure room with restricted access.

Do doors to secure areas automatically unlock in case of a fire or power failure? What security breaches can this cause?



CERT Training and Education

## Network and Systems

**Recommendations and considerations include**

- **separate CSIRT network**
- **separate email, web, DNS, and other appropriate servers and services**
- **up-to-date and consistent software versions and patches**
- **secure network and system configurations**
- **method for updating software on staff devices in a standardized fashion**
- **guidelines on appropriate software to use and not use**
- **test network, lab, or devices**
- **secure intranet for CSIRT staff**

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.

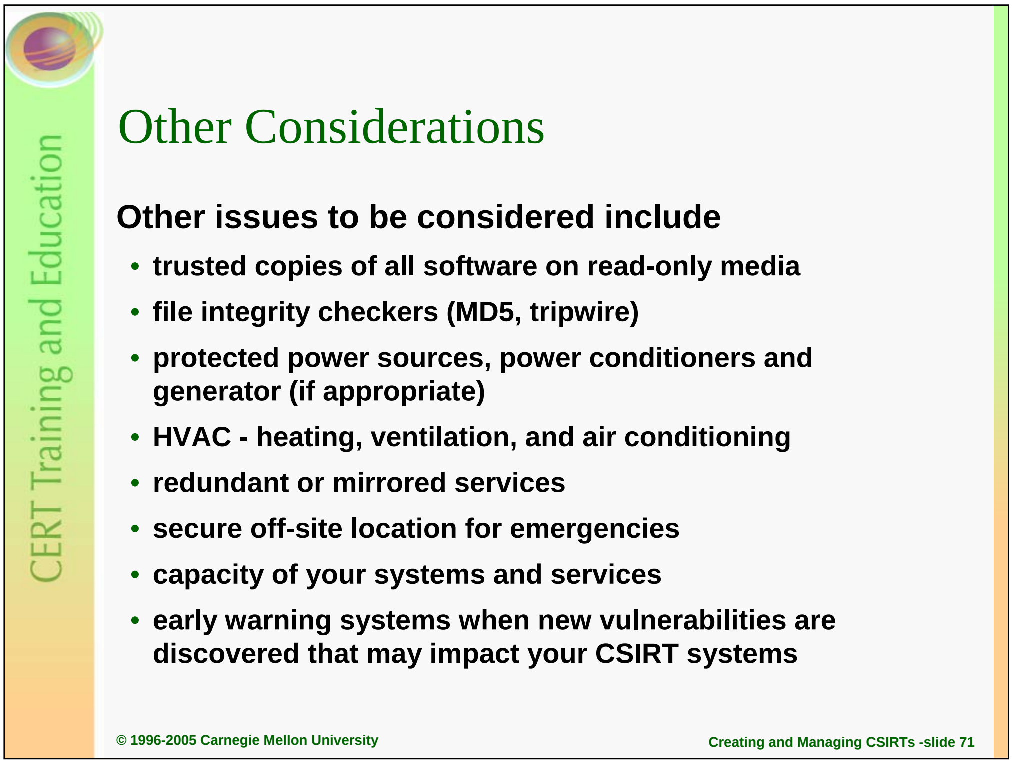
- Configure hosts and network devices (routers, switches, hubs, firewalls, etc.) securely.
- Limit access through access control lists (ACLs) on hosts and network devices.
- Configure monitoring, auditing, and logging facilities.
- Secure all media (floppy disks, tapes, etc.).

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



CERT Training and Education

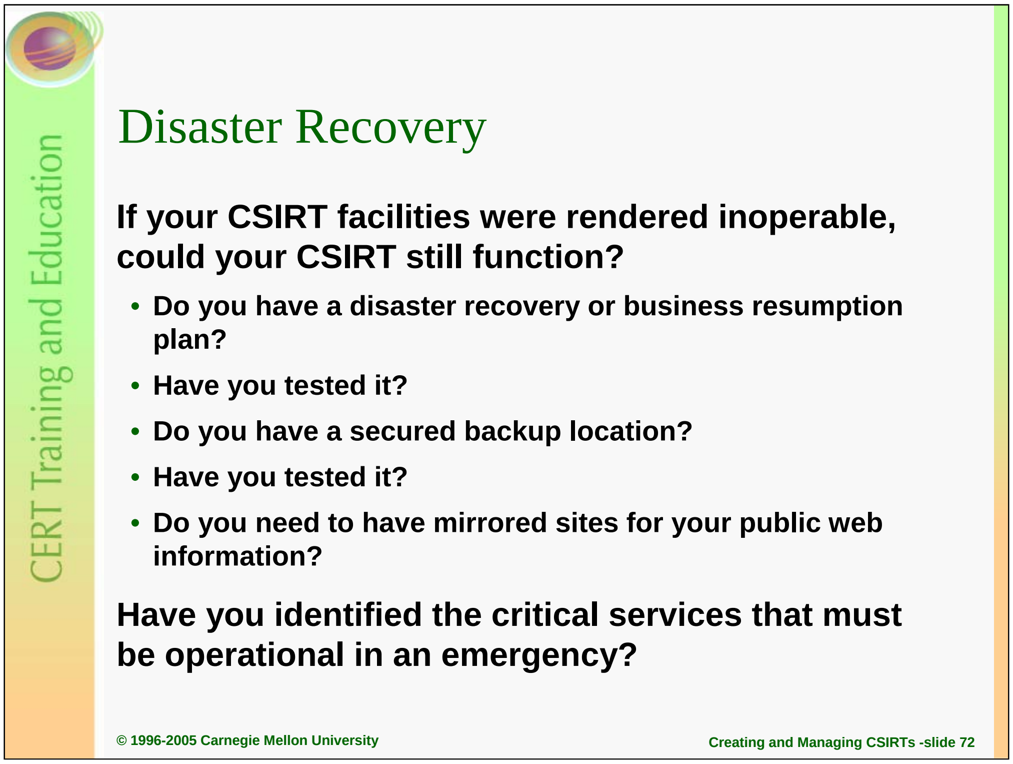
## Other Considerations

**Other issues to be considered include**

- **trusted copies of all software on read-only media**
- **file integrity checkers (MD5, tripwire)**
- **protected power sources, power conditioners and generator (if appropriate)**
- **HVAC - heating, ventilation, and air conditioning**
- **redundant or mirrored services**
- **secure off-site location for emergencies**
- **capacity of your systems and services**
- **early warning systems when new vulnerabilities are discovered that may impact your CSIRT systems**

In regards to the capacity of your systems

- Can your email, web, and other public services stay operational if under a denial of service attack?
- Can your email, web, and other public services stay operational if your constituency is sending large volumes of email and visiting your web site to obtain advisories or patches?


CERT Training and Education

## Disaster Recovery

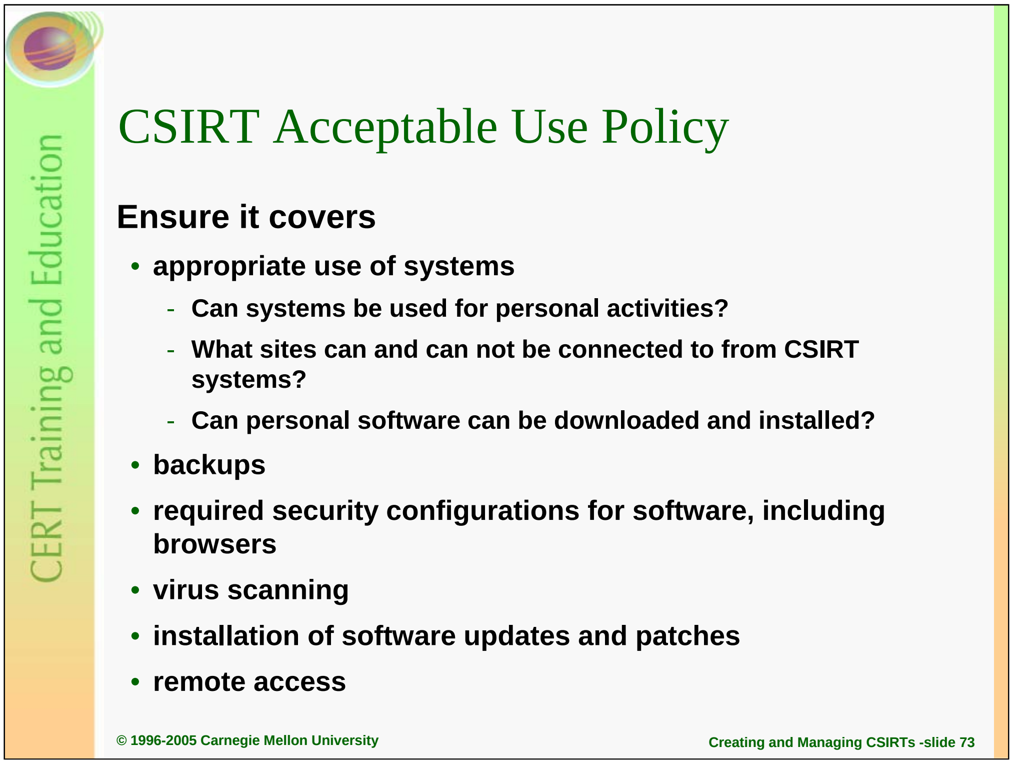
**If your CSIRT facilities were rendered inoperable, could your CSIRT still function?**

- **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 need to have mirrored sites for your public web information?**

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

Creating and Managing CSIRTs -slide 72

You may want to make arrangements with other trusted CSIRTs to mirror important public services you provide.



CERT Training and Education

## CSIRT Acceptable Use Policy

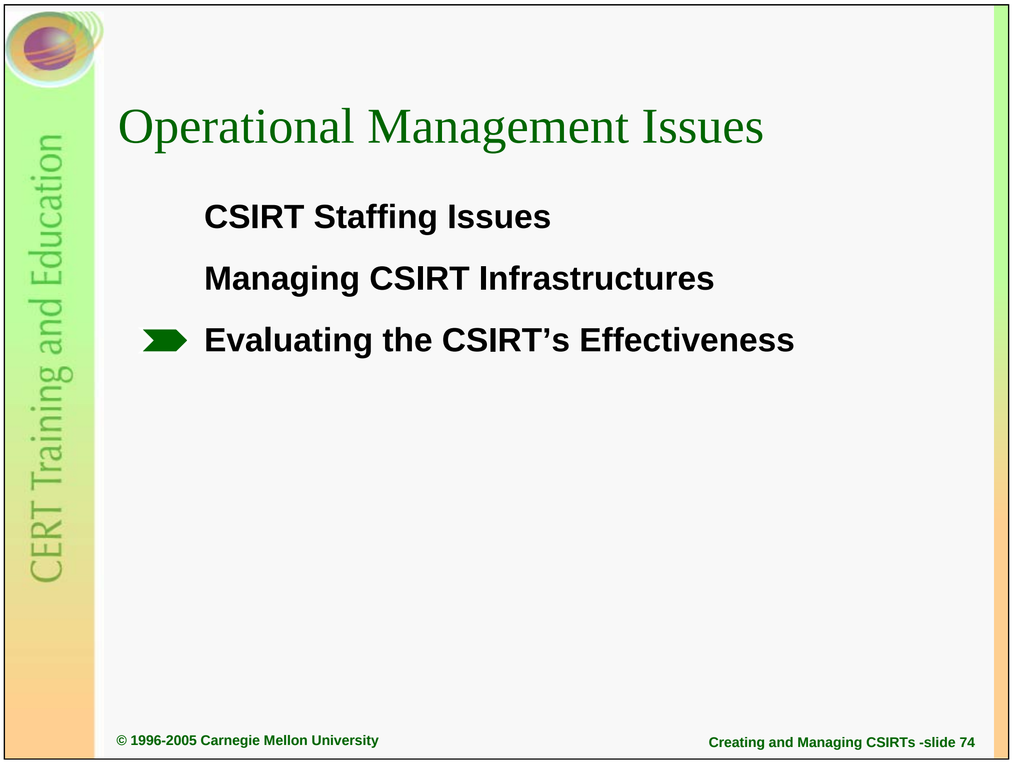
**Ensure it covers**

- **appropriate use of systems**
  - **Can systems be used for personal activities?**
  - **What sites can and can not be connected to from CSIRT systems?**
  - **Can personal software can be downloaded and installed?**
- **backups**
- **required security configurations for software, including browsers**
- **virus scanning**
- **installation of software updates and patches**
- **remote access**

Creating and Managing CSIRTs -slide 73

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?



CERT Training and Education

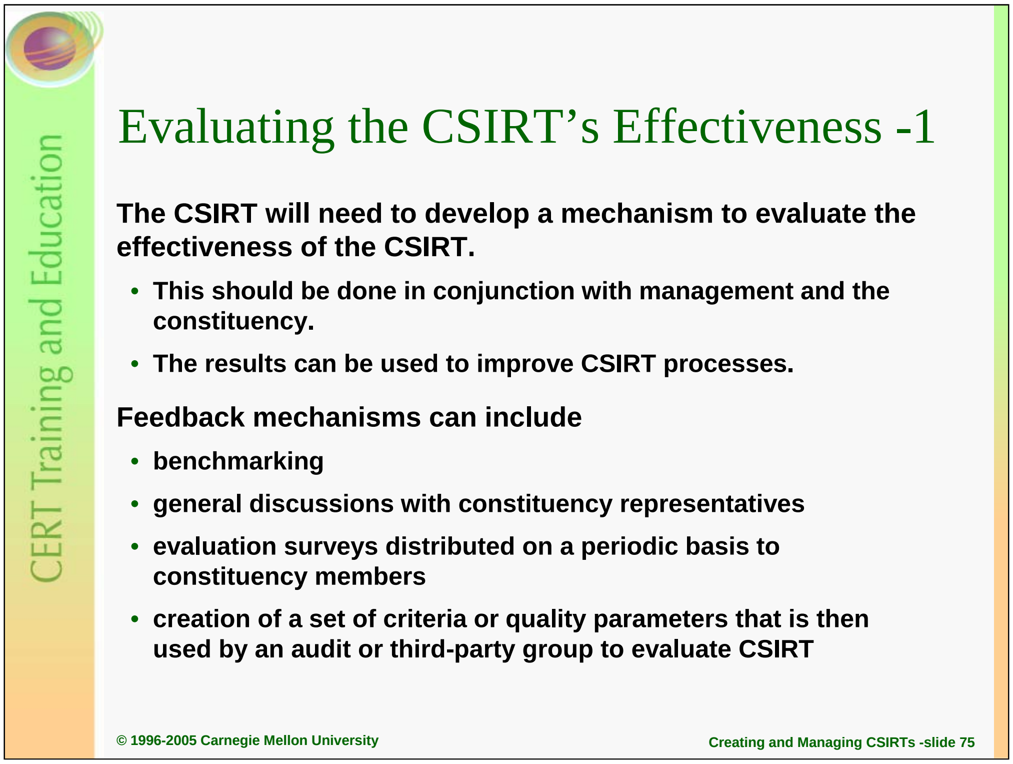
# Operational Management Issues

CSIRT Staffing Issues

Managing CSIRT Infrastructures

➤ Evaluating the CSIRT’s Effectiveness

Creating and Managing CSIRTs -slide 74


CERT Training and Education

## Evaluating the CSIRT’s Effectiveness -1

**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.**

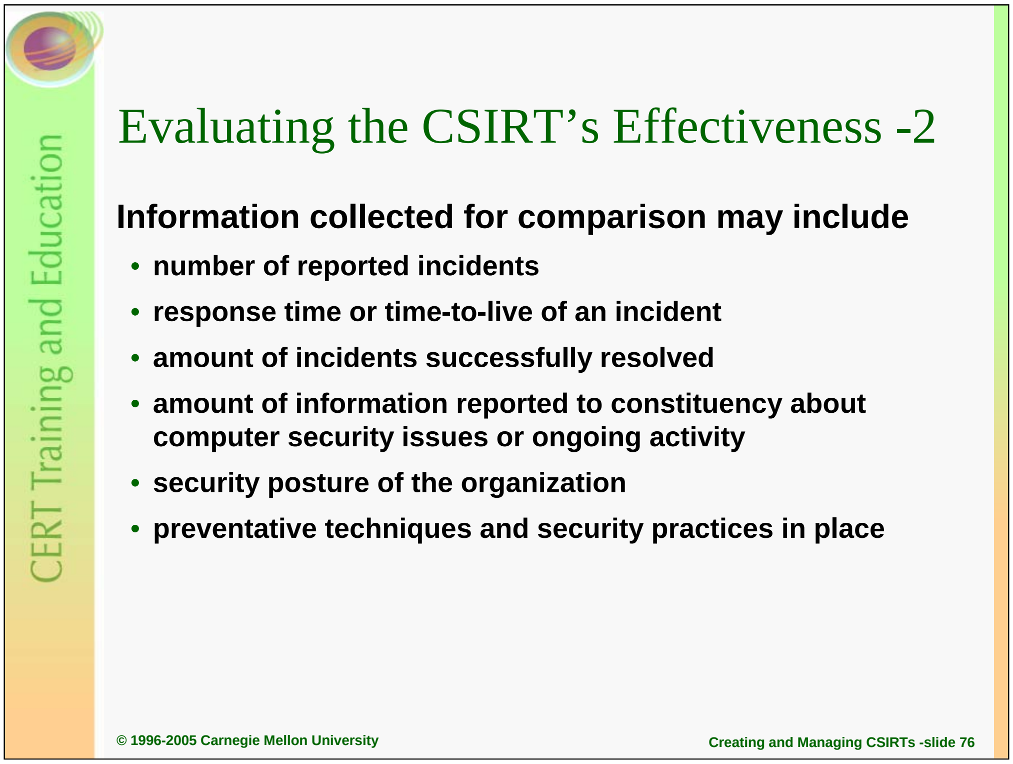
**Feedback mechanisms can include**

- **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**

Creating and Managing CSIRTs -slide 75

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.



CERT Training and Education

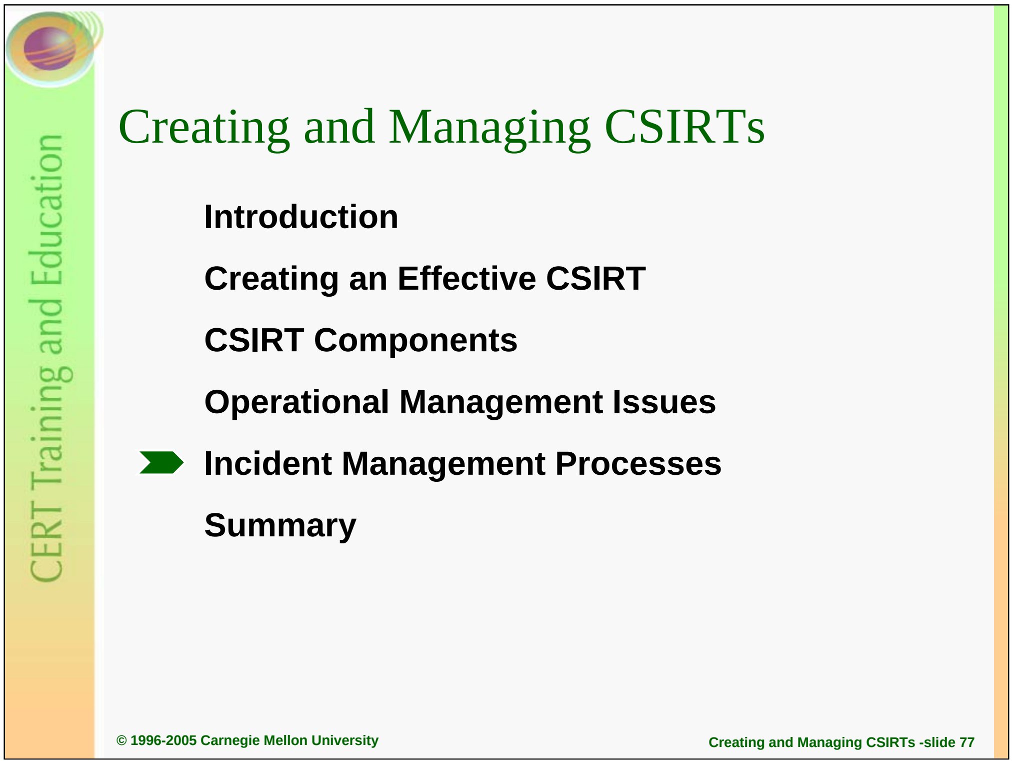
## Evaluating the CSIRT’s Effectiveness -2

**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**

Creating and Managing CSIRTs -slide 76

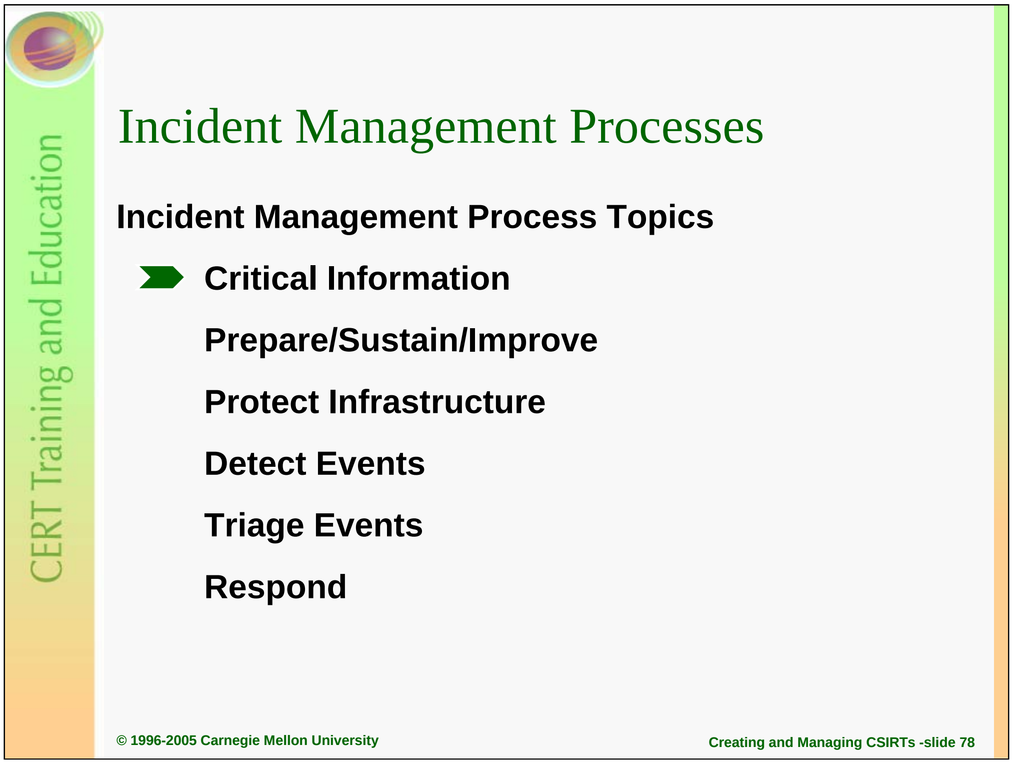
It may be helpful to have previously collected information on the state of the constituency or organization before the implementation of the team. This information can be used as a baseline in determining the effect of the CSIRT on the constituency.



CERT Training and Education

# Creating and Managing CSIRTs

- Introduction
- Creating an Effective CSIRT
- CSIRT Components
- Operational Management Issues
- ➤ Incident Management Processes
- Summary

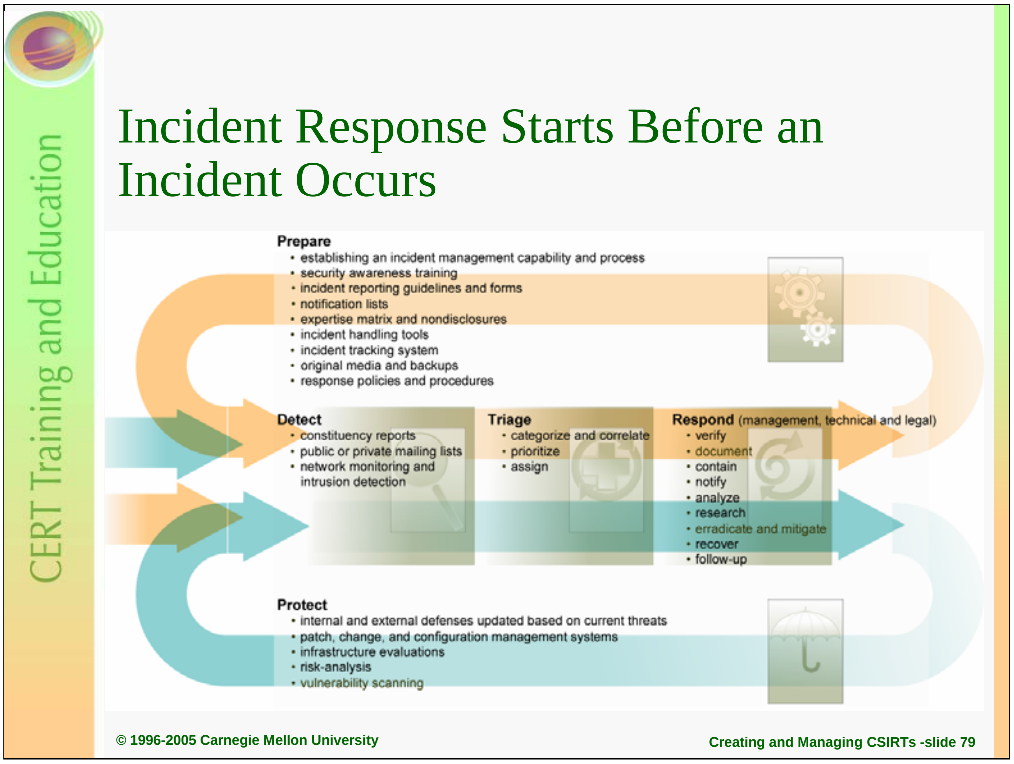


CERT Training and Education

# Incident Management Processes

**Incident Management Process Topics**

- ➤ **Critical Information**
- **Prepare/Sustain/Improve**
- **Protect Infrastructure**
- **Detect Events**
- **Triage Events**
- **Respond**



CERT Training and Education

# Incident Response Starts Before an Incident Occurs

**Prepare**
- establishing an incident management capability and process
- security awareness training
- incident reporting guidelines and forms
- notification lists
- expertise matrix and nondisclosures
- incident handling tools
- incident tracking system
- original media and backups
- response policies and procedures

**Detect**
- constituency reports
- public or private mailing lists
- network monitoring and intrusion detection

**Triage**
- categorize and correlate
- prioritize
- assign

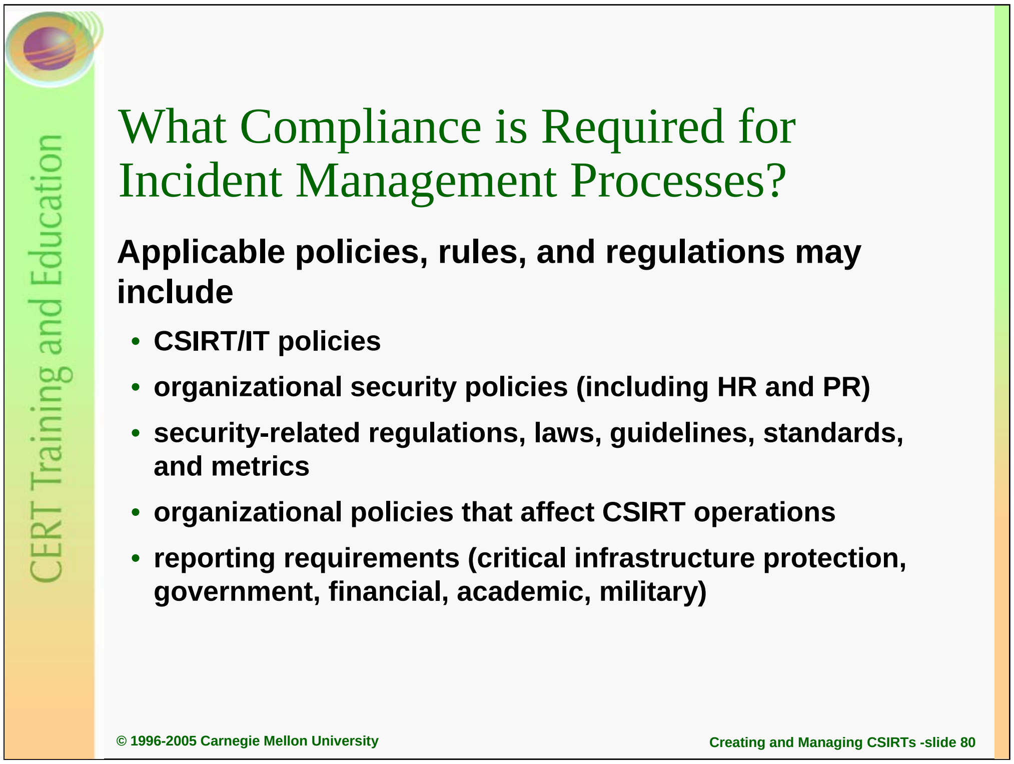
**Respond** (management, technical and legal)
- verify
- document
- contain
- notify
- analyze
- research
- erradicate and mitigate
- recover
- follow-up

**Protect**
- internal and external defenses updated based on current threats
- patch, change, and configuration management systems
- infrastructure evaluations
- risk-analysis
- vulnerability scanning

Creating and Managing CSIRTs -slide 79

Effective response starts long before you actually have an incident to handle. Proactively you can aid the response process by having people, processes, tools, and resources 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.


CERT Training and Education

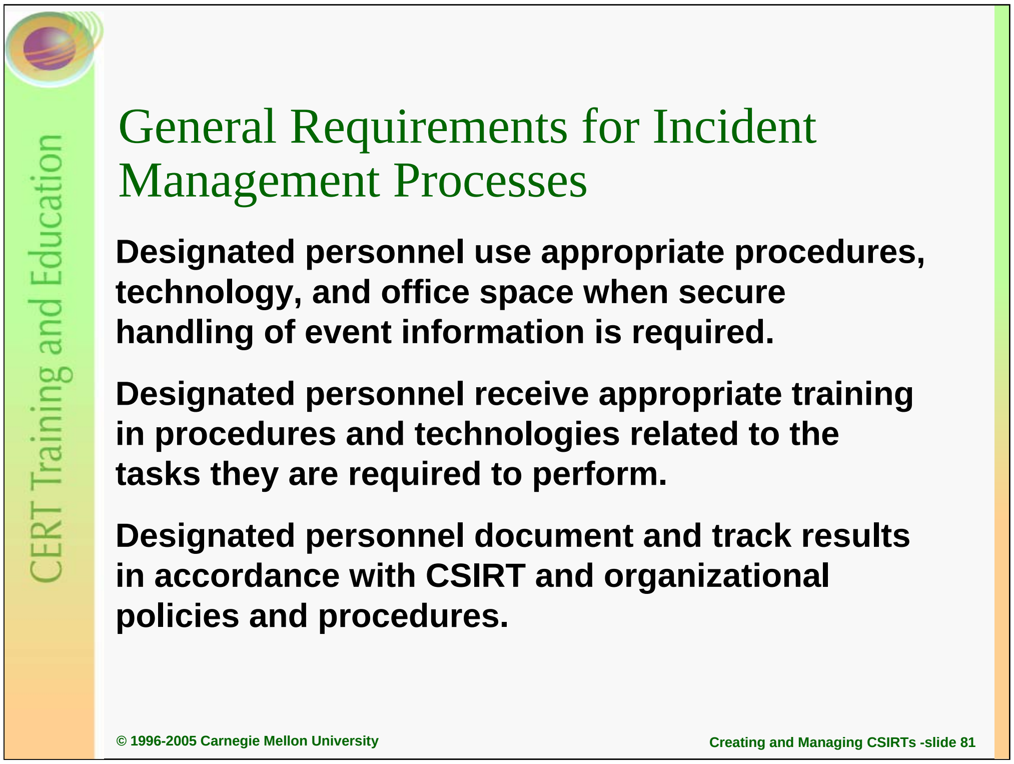
## What Compliance is Required for Incident Management Processes?

**Applicable policies, rules, and regulations may include**

- **CSIRT/IT policies**
- **organizational security policies (including HR and PR)**
- **security-related regulations, laws, guidelines, standards, and metrics**
- **organizational policies that affect CSIRT operations**
- **reporting requirements (critical infrastructure protection, government, financial, academic, military)**

In an educational institution this may include laws and regulations involving

- data protection requirements
- privacy
- copyright

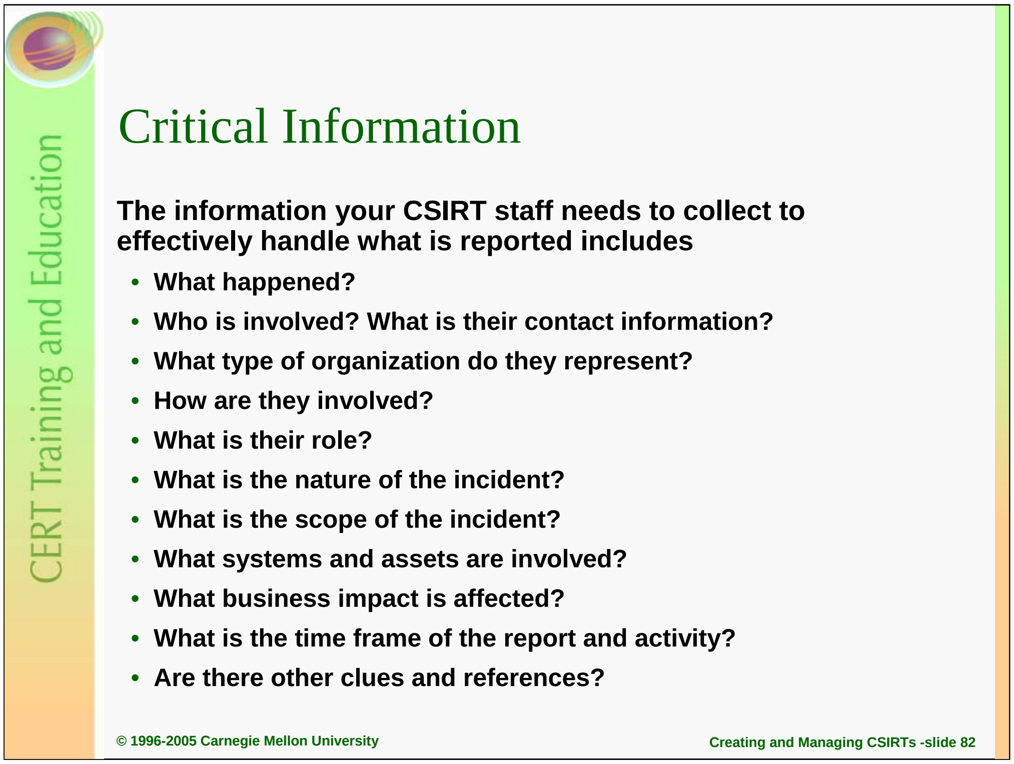

CERT Training and Education

## General Requirements for Incident Management Processes

Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required.

Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Designated personnel document and track results in accordance with CSIRT and organizational policies and procedures.


CERT Training and Education

## Critical Information

**The information your CSIRT staff needs to collect to effectively handle what is reported includes**

- **What happened?**
- **Who is involved? What is their contact information?**
- **What type of organization do they represent?**
- **How are they involved?**
- **What is their role?**
- **What is the nature of the incident?**
- **What is the scope of the incident?**
- **What systems and assets are involved?**
- **What business impact is affected?**
- **What is the time frame of the report and activity?**
- **Are there other clues and references?**

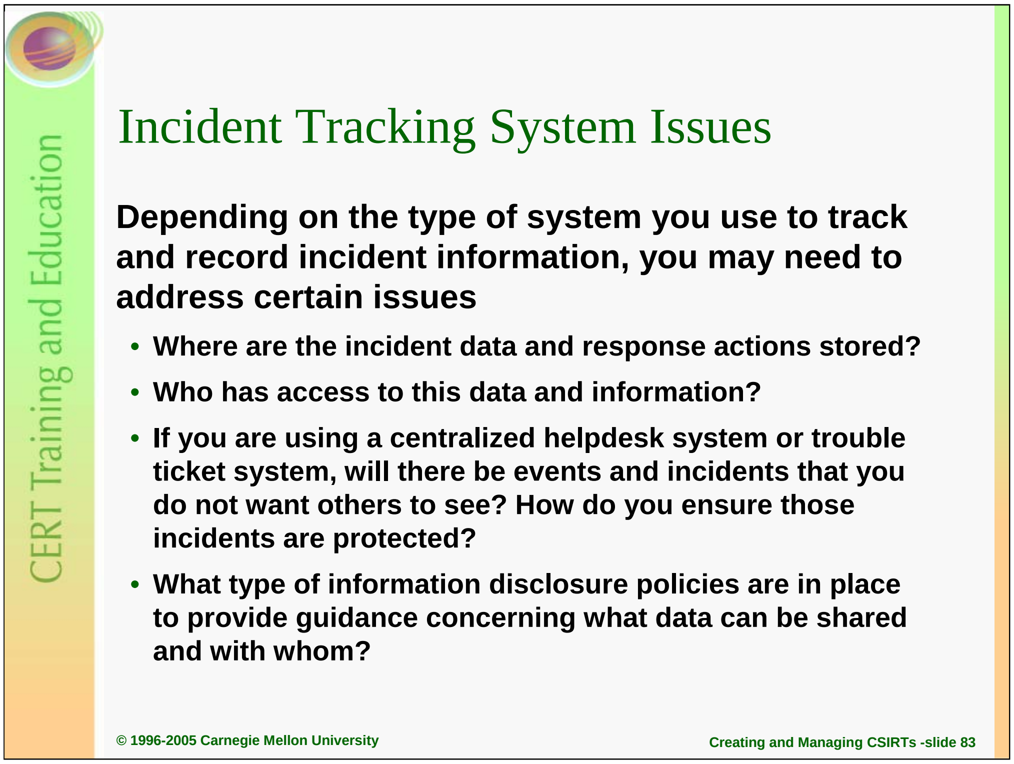
Creating and Managing CSIRTs -slide 82

For information on systems affected, you would want to know the

- purpose of the systems
- criticality of the system
- uptime requirements of the system
- IP address
- hostname
- MAC address
- OS or application version and patch level

It is also important for your staff to identify any items that are

- missing
- incomplete
- incorrect
- relevant (or irrelevant)
- not supported with evidence

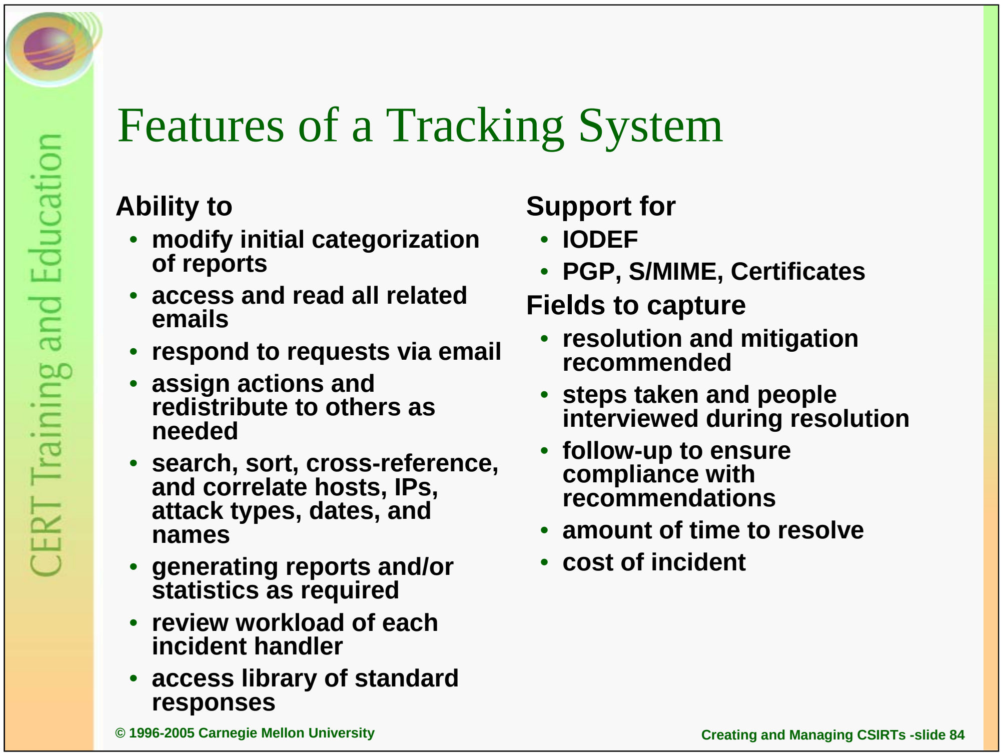


CERT Training and Education

## Incident Tracking System Issues

**Depending on the type of system you use to track and record incident information, you may need to address certain issues**

- **Where are the incident data and response actions stored?**
- **Who has access to this data and information?**
- **If you are using a centralized helpdesk system or trouble ticket system, will there be events and incidents that you do not want others to see? How do you ensure those incidents are protected?**
- **What type of information disclosure policies are in place to provide guidance concerning what data can be shared and with whom?**



CERT Training and Education

## Features of a Tracking System

**Ability to**

- **modify initial categorization of reports**
- **access and read all related emails**
- **respond to requests via email**
- **assign actions and redistribute to others as needed**
- **search, sort, cross-reference, and correlate hosts, IPs, attack types, dates, and names**
- **generating reports and/or statistics as required**
- **review workload of each incident handler**
- **access library of standard responses**

**Support for**

- **IODEF**
- **PGP, S/MIME, Certificates**

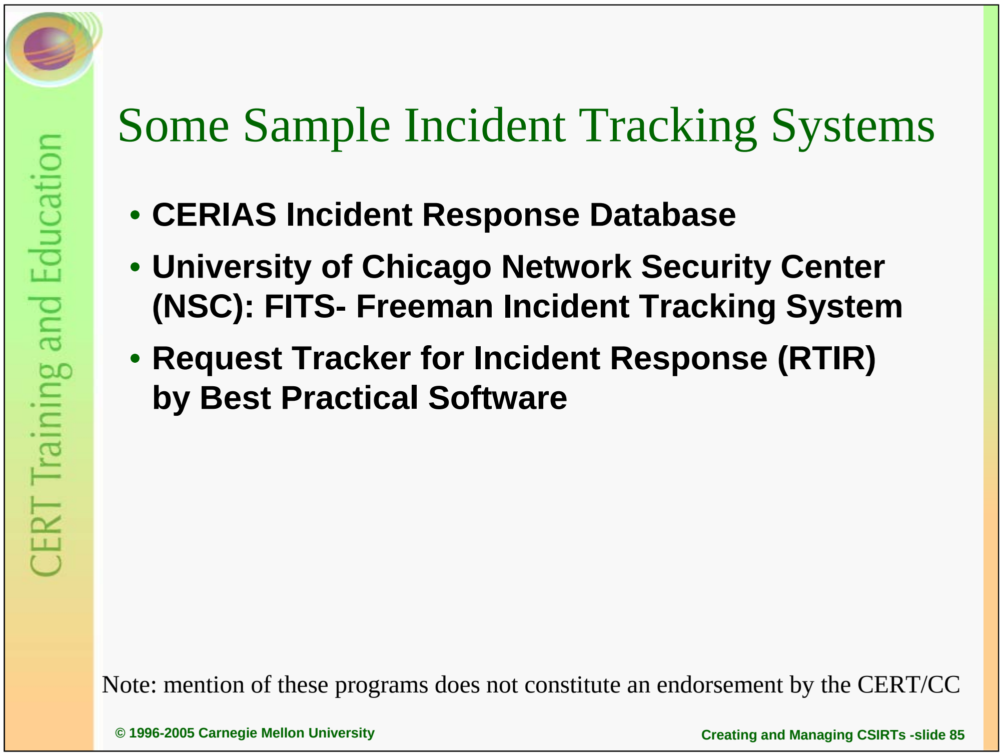
**Fields to capture**

- **resolution and mitigation recommended**
- **steps taken and people interviewed during resolution**
- **follow-up to ensure compliance with recommendations**
- **amount of time to resolve**
- **cost of incident**

Creating and Managing CSIRTs -slide 84

Some of these features may be the same as those required in Triage. The triage systems and the incident tracking system may even be the same system. This usually works better than two separate systems.

The above list is not complete or comprehensive but some examples of information to be tracked and recorded.



CERT Training and Education

## Some Sample Incident Tracking Systems

- CERIAS Incident Response Database
- University of Chicago Network Security Center (NSC): FITS- Freeman Incident Tracking System
- Request Tracker for Incident Response (RTIR) by Best Practical Software

Note: mention of these programs does not constitute an endorsement by the CERT/CC

CERIAS Incident Response Database

- web-based system
- used to collect costs of incident during response
- in development, but available for download

https://cirdb.cerias.purdue.edu/website/

University of Chicago Network Security Center (NSC): FITS- Freeman Incident Tracking System

- uses UNIX file system
- available for download

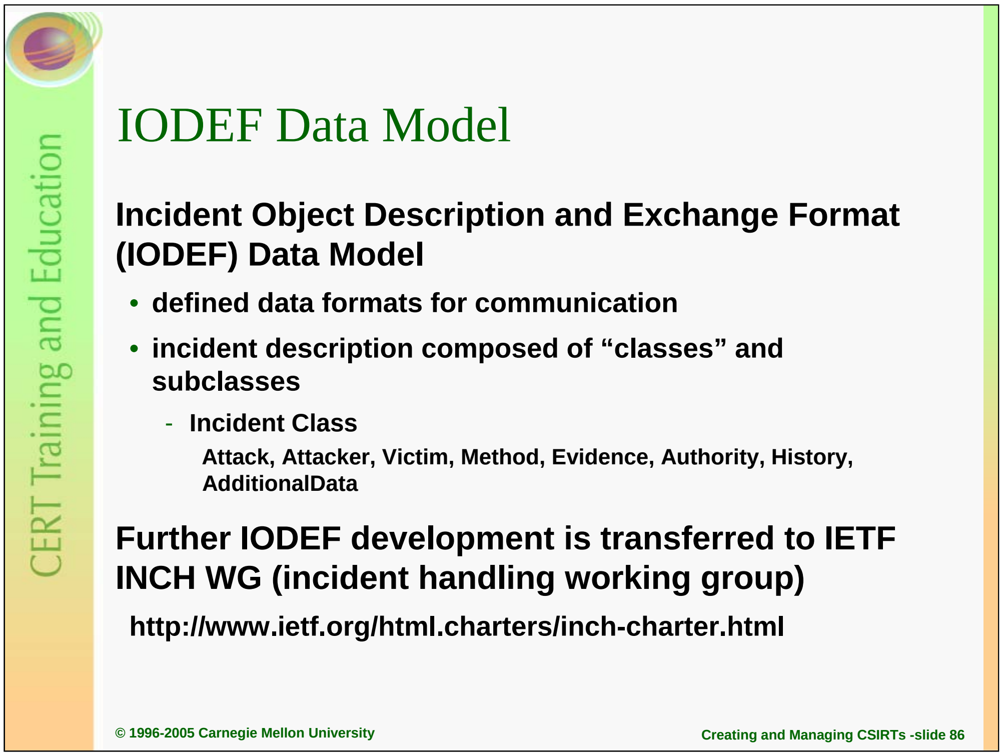
http://security.uchicago.edu/tools/fits/

Request Tracker for Incident Response (RTIR) by Best Practical Software

- web-based system
- customized tracking systems for incident response
- in development, but available for download
- software is free, there are fees for service

http://www.bestpractical.com/rtir/

Several CSIRTs are building their own modules or plug-ins for the RTIR software including JANET-CERT and DFN-CERT.



CERT Training and Education

# IODEF Data Model

**Incident Object Description and Exchange Format (IODEF) Data Model**

- **defined data formats for communication**
- **incident description composed of “classes” and subclasses**
  - **Incident Class**

    **Attack, Attacker, Victim, Method, Evidence, Authority, History, AdditionalData**

**Further IODEF development is transferred to IETF INCH WG (incident handling working group)**

**http://www.ietf.org/html.charters/inch-charter.html**

Creating and Managing CSIRTs -slide 86

The Incident Object Description and Exchange Format (IODEF) Data Model was created out of a working group, initially established under the TF-CSIRT, “to define a common data format and common exchange procedures for sharing information needed to handle an incident between different CSIRTs and to exchange incident related data between CSIRTs that allow both known and new types of incidents to be formatted and exchanged.”

http://www.terena.nl/tech/task-forces/tf-csirt/iodef/

RFC 3067 – “TERENA's Incident Object Description and Exchange Format Requirements”

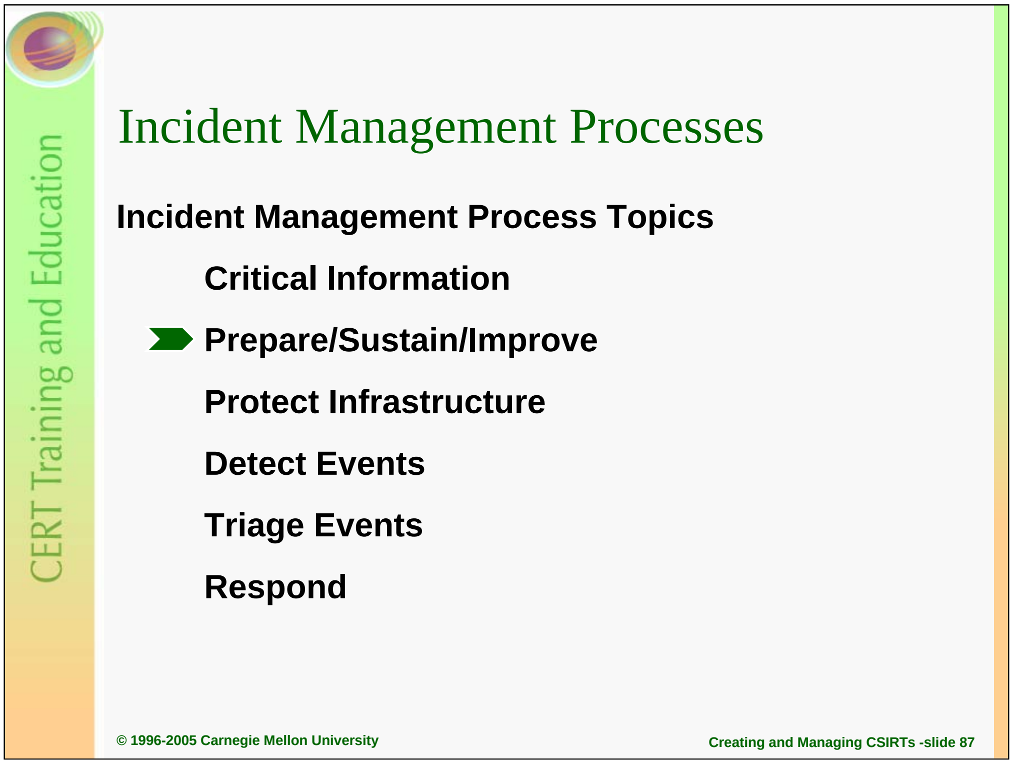
That working group is closed, and further IODEF development has been transferred to the IETF INCH WG (incident handling working group)

http://www.ietf.org/html.charters/inch-charter.html

The IODEF Data Model provides a means to describe an incident by its component “classes” and subclasses, which are defined in the model. The “Incident Class” is composed of several aggregate sub-classes: Attack, Attacker, Victim, Method, Evidence, Authority, History, and AdditionalData. Each of these aggregate classes (or sub-classes) has its own attributes that contain information about the security events that constitute the incident. (For example, the “Attack” class is constituted of aggregate classes: Source, Target, Description, DetectTime, StartTime, and EndTime. Each of these aggregate classes is composed of additional aggregate classes.)

For more information, see the latest Internet Draft available at

http://www.ietf.org/html.charters/inch-charter.html
“Incident Object Description Exchange Format Data Model and XML Implementation”



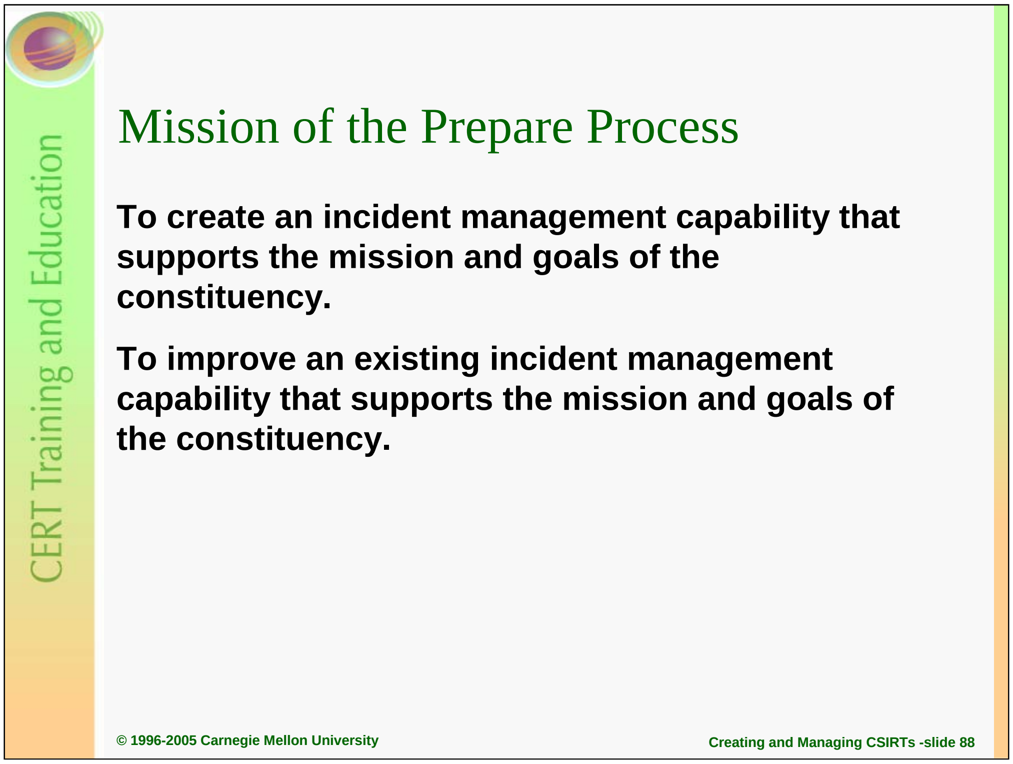
CERT Training and Education

## Incident Management Processes

**Incident Management Process Topics**

- **Critical Information**
- ➤ **Prepare/Sustain/Improve**
- **Protect Infrastructure**
- **Detect Events**
- **Triage Events**
- **Respond**

Creating and Managing CSIRTs -slide 87



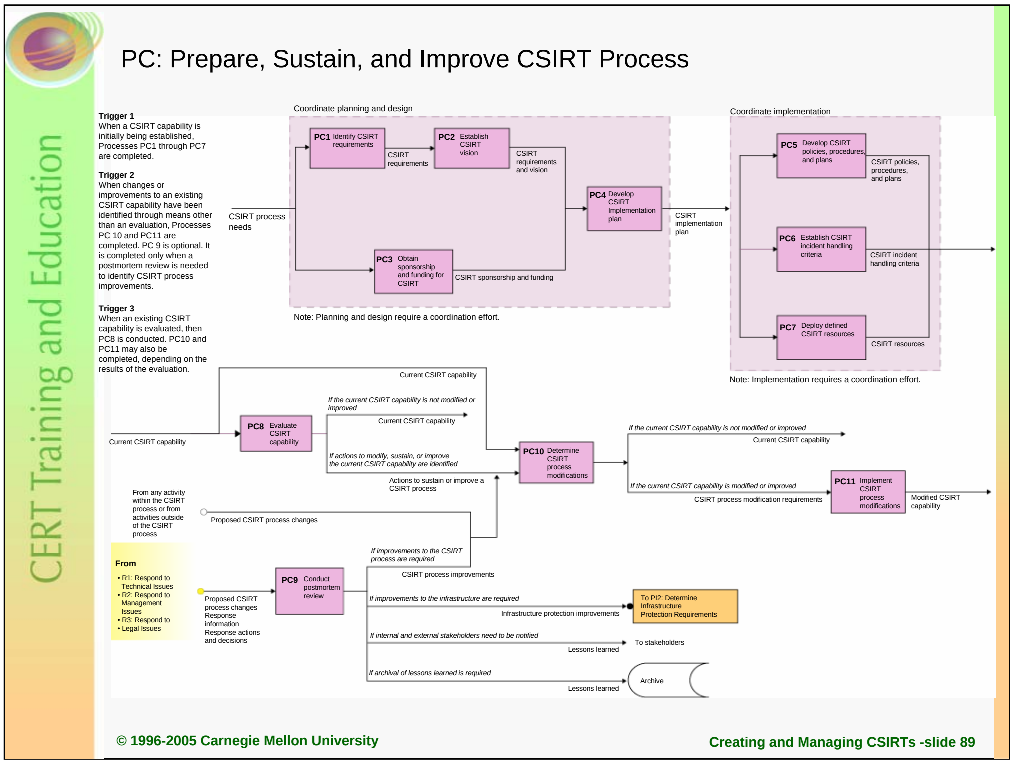
CERT Training and Education

# Mission of the Prepare Process

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

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

Creating and Managing CSIRTs -slide 88



## PC: Prepare, Sustain, and Improve CSIRT Process

CERT Training and Education

**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.

Coordinate planning and design

CSIRT process needs

**PC1** Identify CSIRT requirements

CSIRT requirements

**PC2** Establish CSIRT vision

CSIRT requirements and vision

**PC3** Obtain sponsorship and funding for CSIRT

CSIRT sponsorship and funding

**PC4** Develop CSIRT Implementation plan

CSIRT implementation plan

Note: Planning and design require a coordination effort.

Coordinate implementation

**PC5** Develop CSIRT policies, procedures, and plans

CSIRT policies, procedures, and plans

**PC6** Establish CSIRT incident handling criteria

CSIRT incident handling criteria

**PC7** Deploy defined CSIRT resources

CSIRT resources

Note: Implementation requires a coordination effort.

Current CSIRT capability

**PC8** Evaluate CSIRT capability

Current CSIRT capability

*If the current CSIRT capability is not modified or improved*

Current CSIRT capability

*If actions to modify, sustain, or improve the current CSIRT capability are identified*

Actions to sustain or improve a CSIRT process

**PC10** Determine CSIRT process modifications

*If the current CSIRT capability is not modified or improved*

Current CSIRT capability

*If the current CSIRT capability is modified or improved*

CSIRT process modification requirements

**PC11** Implement CSIRT process modifications

Modified CSIRT capability

From any activity within the CSIRT process or from activities outside of the CSIRT process

Proposed CSIRT process changes

**From**

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

Proposed CSIRT process changes
Response information
Response actions and decisions

**PC9** Conduct postmortem review

*If improvements to the CSIRT process are required*

CSIRT process improvements

*If improvements to the infrastructure are required*

Infrastructure protection improvements

To PI2: Determine Infrastructure Protection Requirements

*If internal and external stakeholders need to be notified*

Lessons learned

To stakeholders

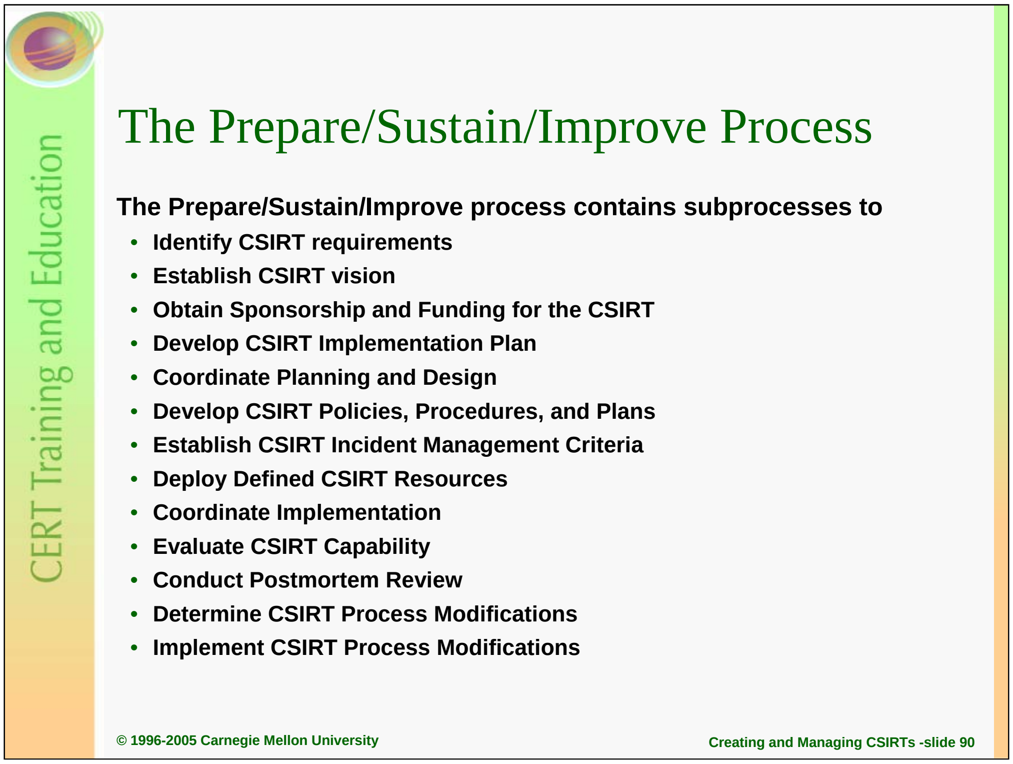
*If archival of lessons learned is required*

Lessons learned

Archive

Processes include

- coordinate planning and design
  - identify CSIRT requirements
  - establish CSIRT vision
  - obtain CSIRT funding and sponsorship
  - develop CSIRT implementation plan
- coordinate implementation
  - develop CSIRT policies, processes, or plans
  - establish CSIRT incident handling criteria
  - implement defined CSIRT resources (staff, equipment and infrastructure)
- evaluate CSIRT capability
- conduct post-mortem review
- determine CSIRT process modifications
- implement CSIRT process modifications


CERT Training and Education

# The Prepare/Sustain/Improve Process

**The Prepare/Sustain/Improve process contains subprocesses to**

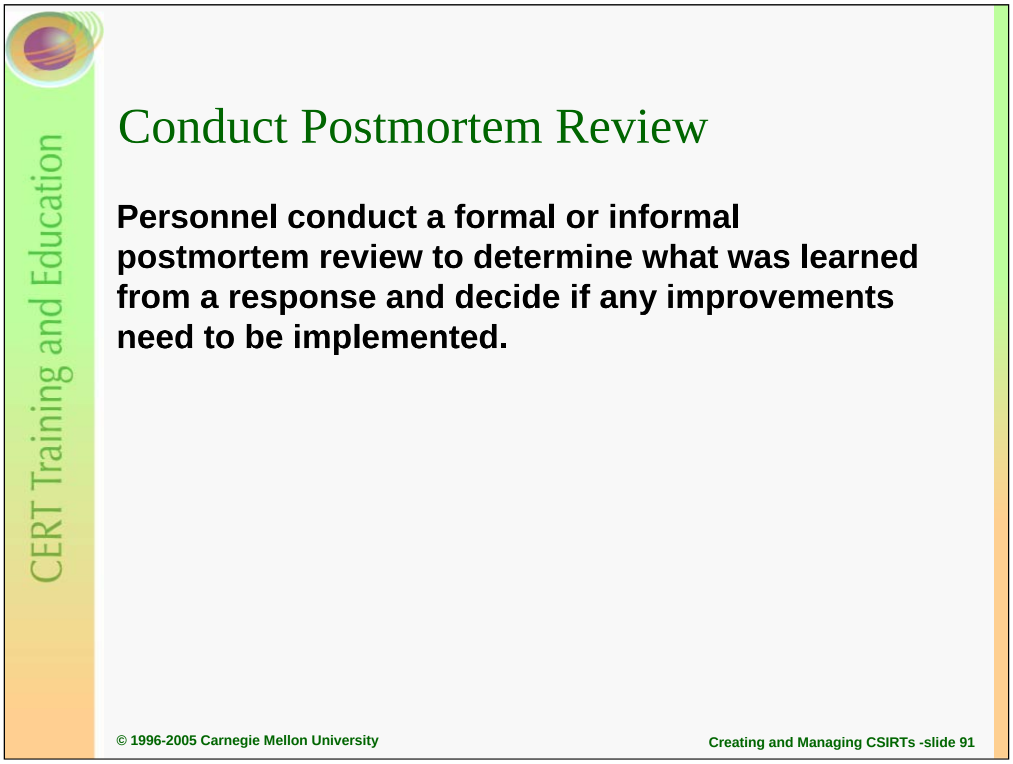
- **Identify CSIRT requirements**
- **Establish CSIRT vision**
- **Obtain Sponsorship and Funding for the CSIRT**
- **Develop CSIRT Implementation Plan**
- **Coordinate Planning and Design**
- **Develop CSIRT Policies, Procedures, and Plans**
- **Establish CSIRT Incident Management Criteria**
- **Deploy Defined CSIRT Resources**
- **Coordinate Implementation**
- **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

We have not talked about doing a postmortem review, that will be discussed on the next slide.



CERT Training and Education

## Conduct Postmortem Review

**Personnel conduct a formal or informal postmortem review to determine what was learned from a response and decide if any improvements need to be implemented.**

Any incident management capability or CSIRT requires a capacity to conduct a postmortem to determine lessons learned and process improvements.

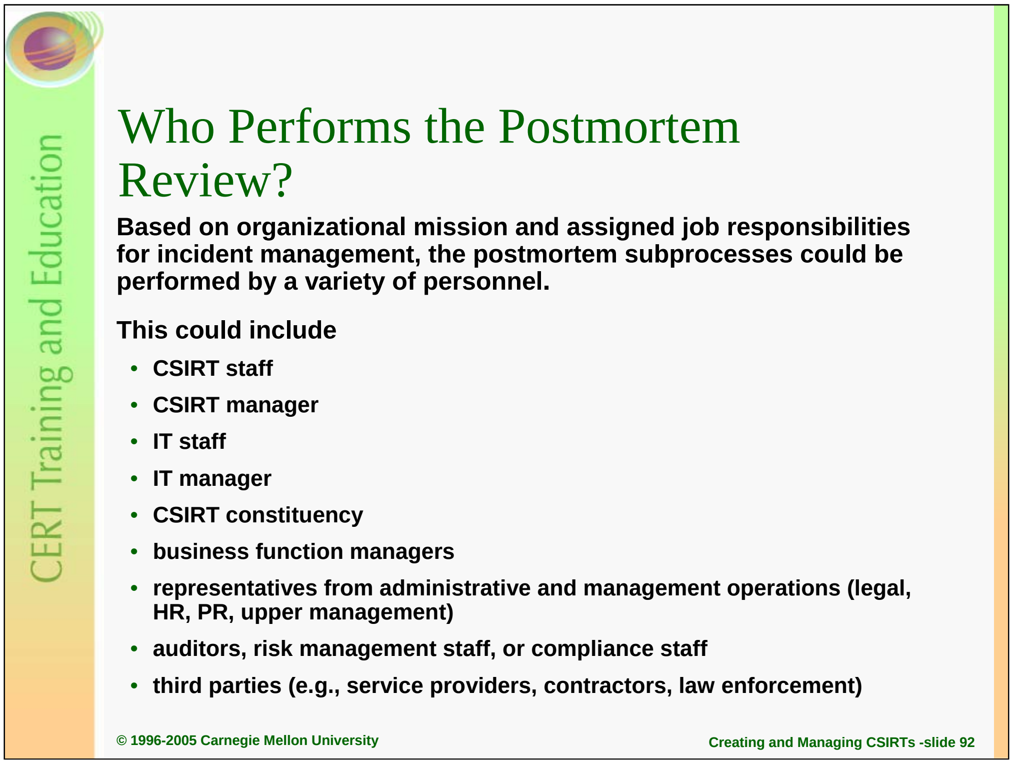
Inputs to the postmortem include

- 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.



CERT Training and Education

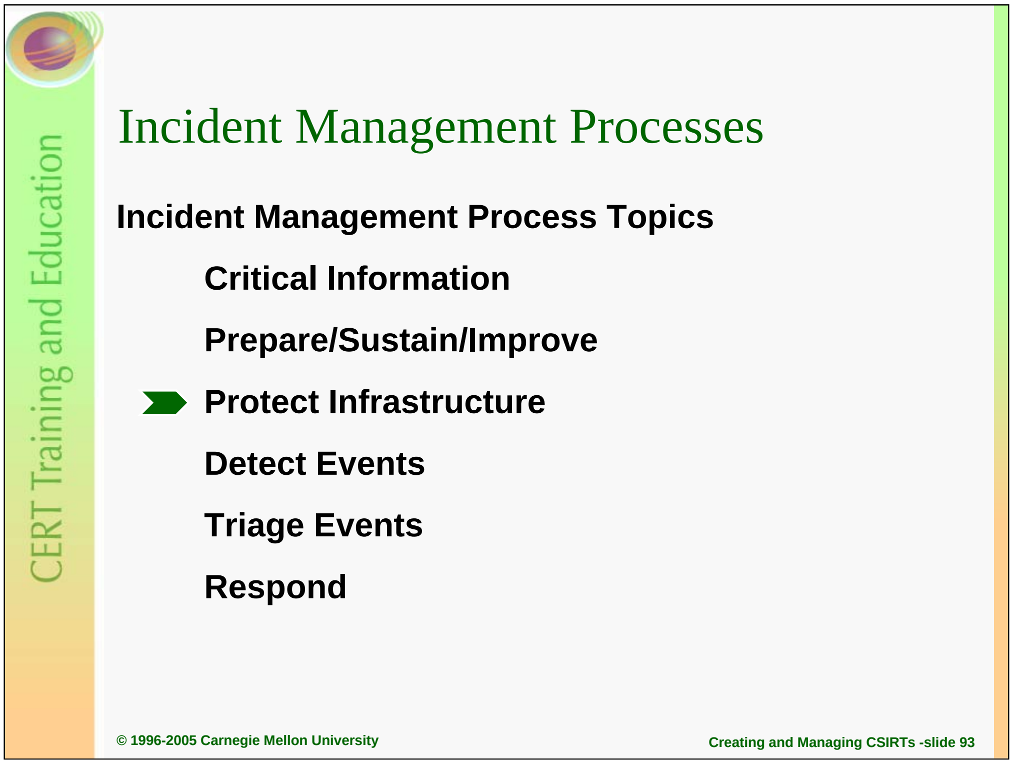
# Who Performs the Postmortem Review?

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

**This could include**

- **CSIRT staff**
- **CSIRT manager**
- **IT staff**
- **IT manager**
- **CSIRT constituency**
- **business function managers**
- **representatives from administrative and management operations (legal, HR, PR, upper management)**
- **auditors, risk management staff, or compliance staff**
- **third parties (e.g., service providers, contractors, law enforcement)**

Ensure all involved are part of the postmortem, especially extended staff and contractors.



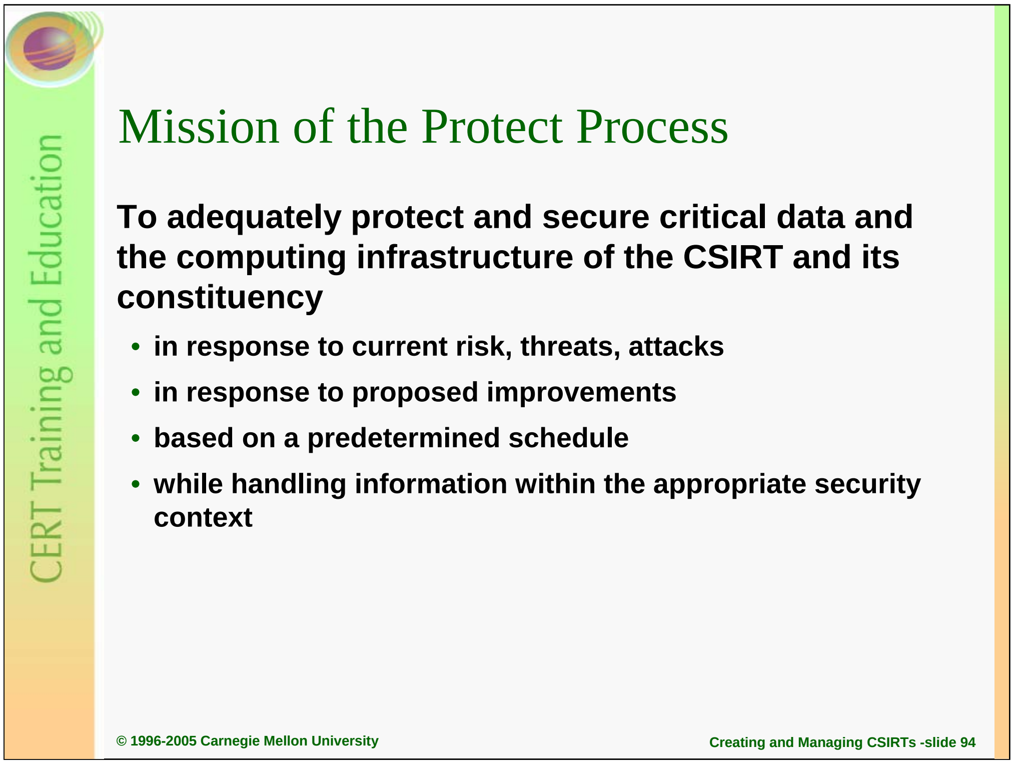
CERT Training and Education

## Incident Management Processes

**Incident Management Process Topics**

- **Critical Information**
- **Prepare/Sustain/Improve**
- ➤ **Protect Infrastructure**
- **Detect Events**
- **Triage Events**
- **Respond**

Creating and Managing CSIRTs -slide 93



CERT Training and Education

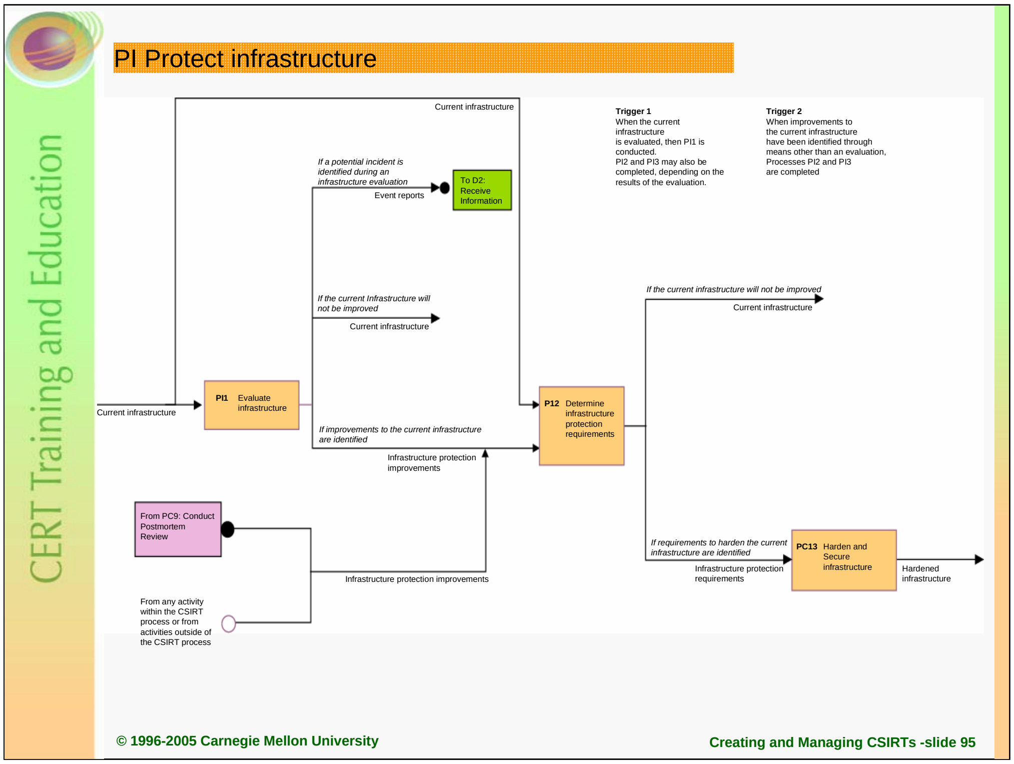
## Mission of the Protect Process

**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



CERT Training and Education

## PI Protect infrastructure

Current infrastructure

PI1 Evaluate infrastructure

Current infrastructure

*If a potential incident is identified during an infrastructure evaluation*

Event reports

To D2: Receive Information

*If the current Infrastructure will not be improved*

Current infrastructure

*If improvements to the current infrastructure are identified*

Infrastructure protection improvements

From PC9: Conduct Postmortem Review

From any activity within the CSIRT process or from activities outside of the CSIRT process

Infrastructure protection improvements

P12 Determine infrastructure protection requirements

*If the current infrastructure will not be improved*

Current infrastructure

*If requirements to harden the current infrastructure are identified*

Infrastructure protection requirements

PC13 Harden and Secure infrastructure

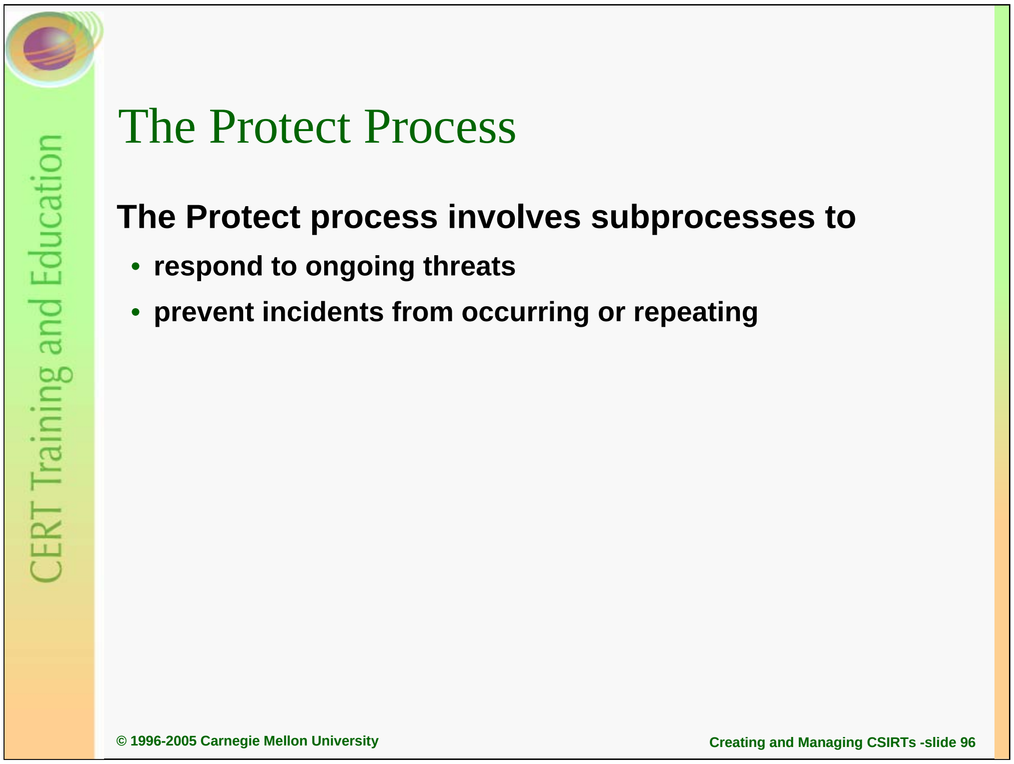
Hardened infrastructure

**Trigger 1**
When the current infrastructure is evaluated, then PI1 is conducted.
PI2 and PI3 may also be completed, depending on the results of the evaluation.

**Trigger 2**
When improvements to the current infrastructure have been identified through means other than an evaluation, Processes PI2 and PI3 are completed

Creating and Managing CSIRTs -slide 95

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 (PI1) 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 (PI2) and implemented as appropriate (PI3).

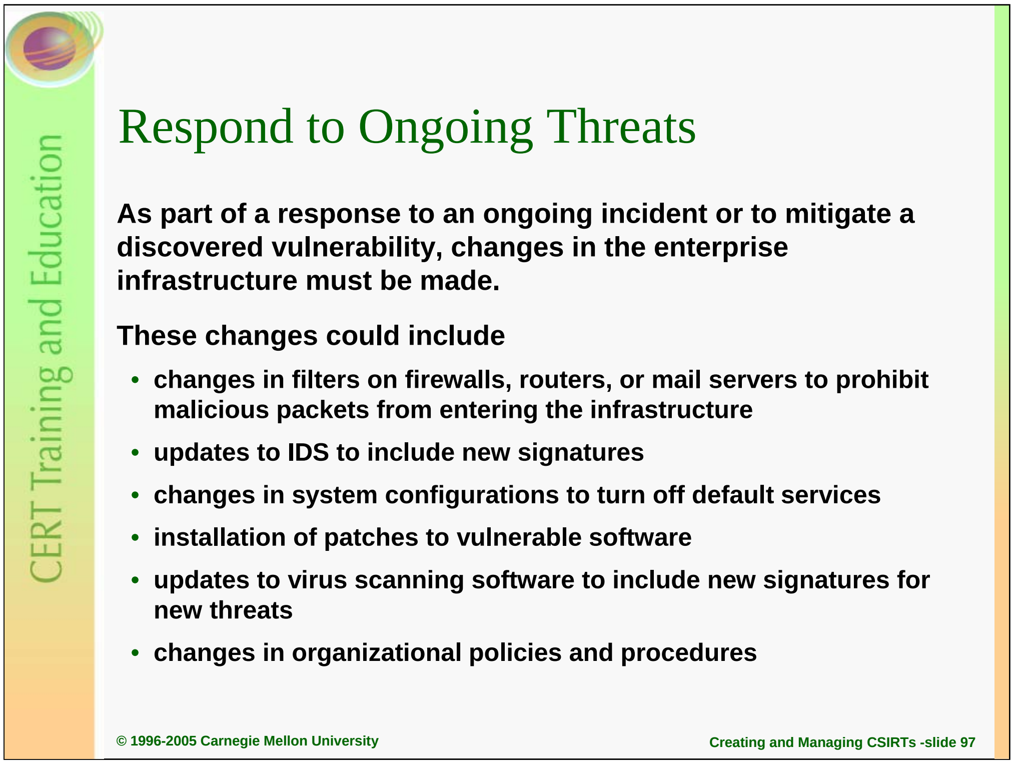


CERT Training and Education

# The Protect Process

**The Protect process involves subprocesses to**

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



CERT Training and Education

## Respond to Ongoing Threats

**As part of a response to an ongoing incident or to mitigate a discovered vulnerability, changes in the enterprise infrastructure must be made.**

**These changes could include**

- **changes in filters on firewalls, routers, or mail servers to prohibit malicious packets from entering the infrastructure**
- **updates to IDS to include new signatures**
- **changes in system configurations to turn off default services**
- **installation of patches to vulnerable software**
- **updates to virus scanning software to include new signatures for new threats**
- **changes in organizational policies and procedures**

Creating and Managing CSIRTs -slide 97

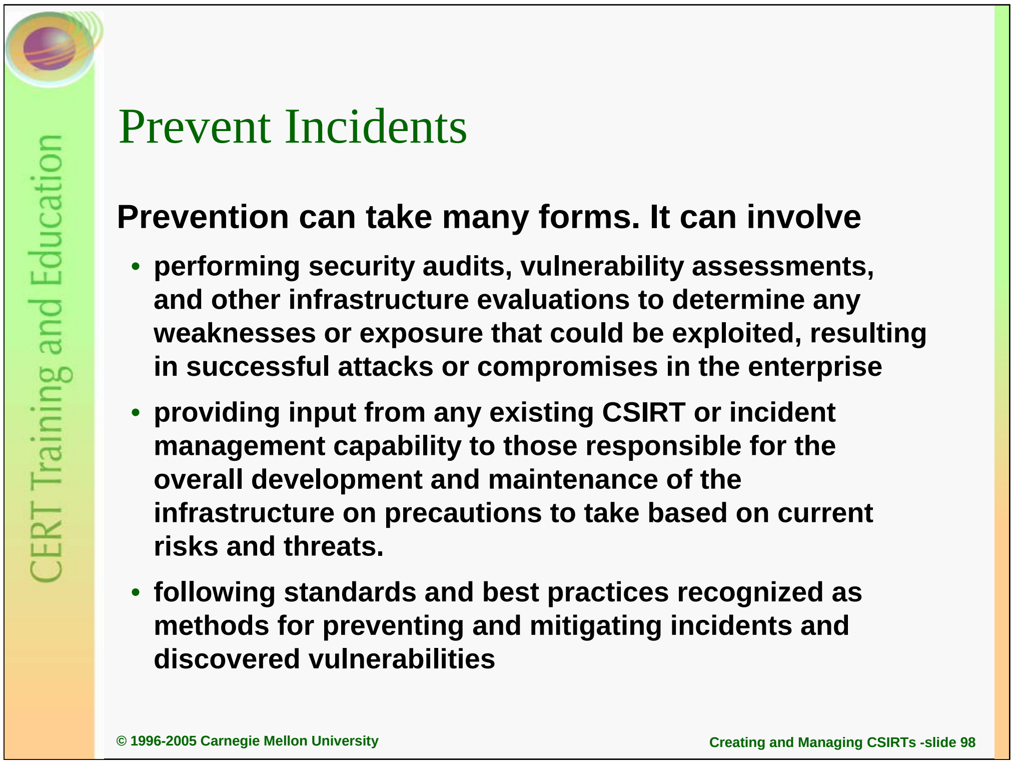
The implementation would include taking any actions to harden and secure the infrastructure. This could result in the addition of or modification to defenses such as firewalls, network monitoring, and IDS. It could result in configuration changes to hosts, servers, routers, firewalls, and other infrastructure components. This can also include changes in policies and procedures related to acceptable use, account management, physical security, human resources, or other similar areas.

Written policies and guidelines that can benefit CSIRT staff, parent organization, and constituency members include

- accounts and password creation and use – selecting good passwords, not sharing accounts and passwords
- software use and installation – how to securely configure systems, how to keep up to date with patches and new software versions, not using software with known problems
- web and email appropriate use – guidance for downloading files or running programs from external sources (e.g., email attachments), avoiding “questionable” sites
- detecting/reporting/responding to an incident – whom to report to, what to report, and how to report

Establish procedures for terminating employees to avoid insider attacks by former employees. Work with your human resources department to establish an acceptable use policy so employees know what they should and should not do.  Work with IT to determine what systems need to be changed and protected when someone leaves.

Ensure you have trusted backups of all applications and data. Have notification lists created and available in both hardcopy and electronic format. Have detection methods in place such as auditing and monitoring of systems and networks. Install file integrity checkers – to help determine what has been changed. Create an incident response analysis toolkit, system, or lab before an event occurs. Ensure there are defined communication and coordination channels established between the CSIRT and any configuration, patch, and change management systems.



CERT Training and Education

## Prevent Incidents

**Prevention can take many forms. It can involve**

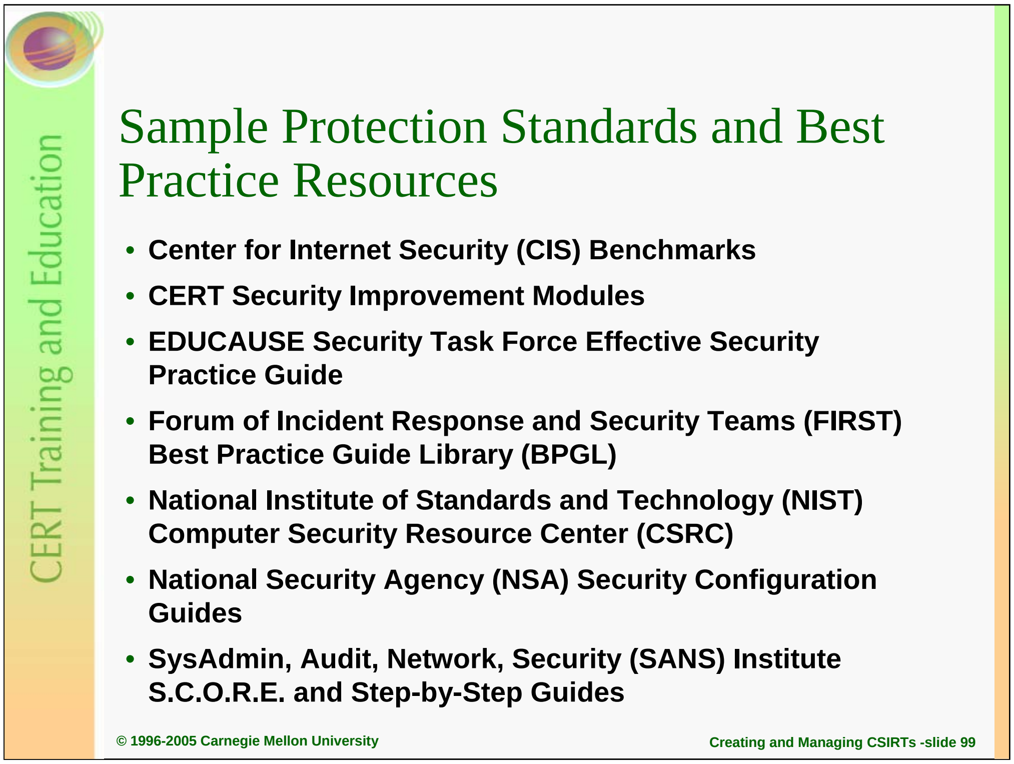
- **performing security audits, vulnerability assessments, and other infrastructure evaluations to determine any weaknesses or exposure that could be exploited, resulting in successful attacks or compromises in the enterprise**
- **providing input from any existing CSIRT or incident management capability to those responsible for the overall development and maintenance of the infrastructure on precautions to take based on current risks and threats.**
- **following standards and best practices recognized as methods for preventing and mitigating incidents and discovered vulnerabilities**

Creating and Managing CSIRTs -slide 98

This last point is basically the implementation of best practices for the protection of systems and networks based on the relevant standard of due care, be it ISO 17799 or other standards or regulatory requirements. Theoretically, improved protection of systems reduces the number of incidents that must be handled.

The following list is a sampling of some of the available standards and best practices that organizations can adhere to that provide guidance for proactively securing and hardening the enterprise infrastructure. Much work has been done in this area, and we do not want to repeat that work here.

- ISO 17799/British Standards Institute 7799 Part 2
- 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



CERT Training and Education

## Sample Protection Standards and Best Practice Resources

- Center for Internet Security (CIS) Benchmarks
- CERT Security Improvement Modules
- EDUCAUSE Security Task Force Effective Security Practice Guide
- Forum of Incident Response and Security Teams (FIRST) Best Practice Guide Library (BPGL)
- National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC)
- National Security Agency (NSA) Security Configuration Guides
- SysAdmin, Audit, Network, Security (SANS) Institute S.C.O.R.E. and Step-by-Step Guides

CIS Benchmarks
http://www.cisecurity.org/benchmarks.html

CERT Security Improvement Modules
http://www.cert.org/security-improvement/

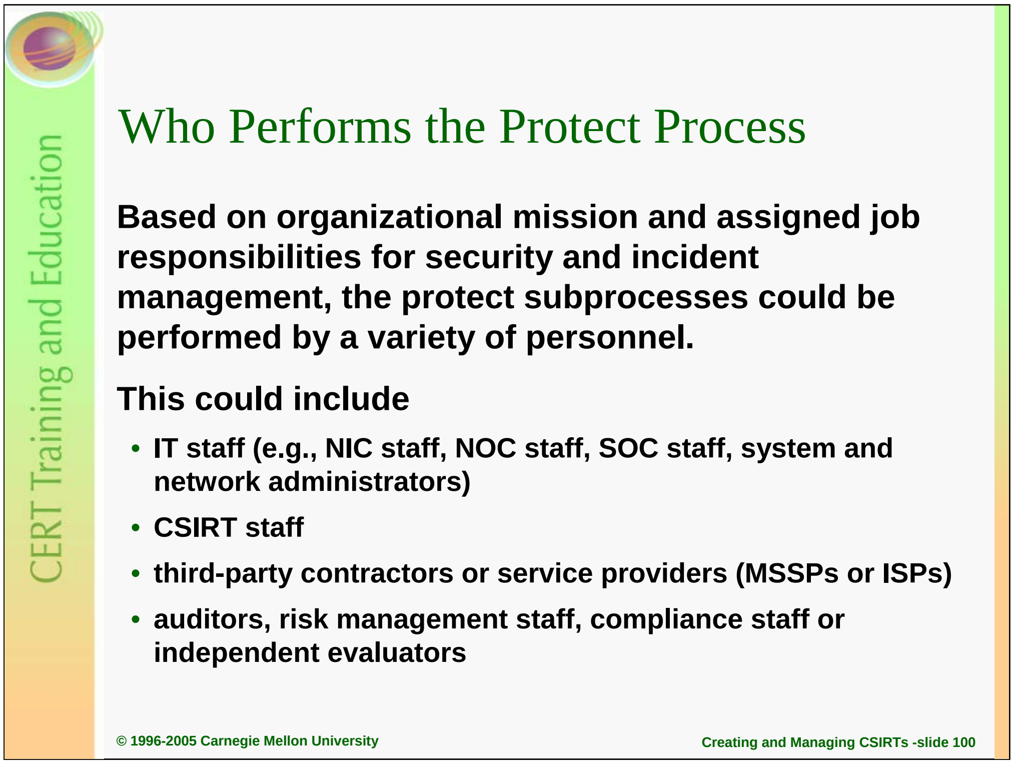
EDUCAUSE – Security Task Force
http://www.educause.edu/security

FIRST Best Practice Guide Library (BPGL)
http://www.first.org/resources/guides/

NIST Computer Security Resource Center
http://csrc.nist.gov/

NSA Security Configuration Guides
http://www.nsa.gov/snac/

SANS S.C.O.R.E.
http://www.sans.org/score/



CERT Training and Education

## Who Performs the Protect Process

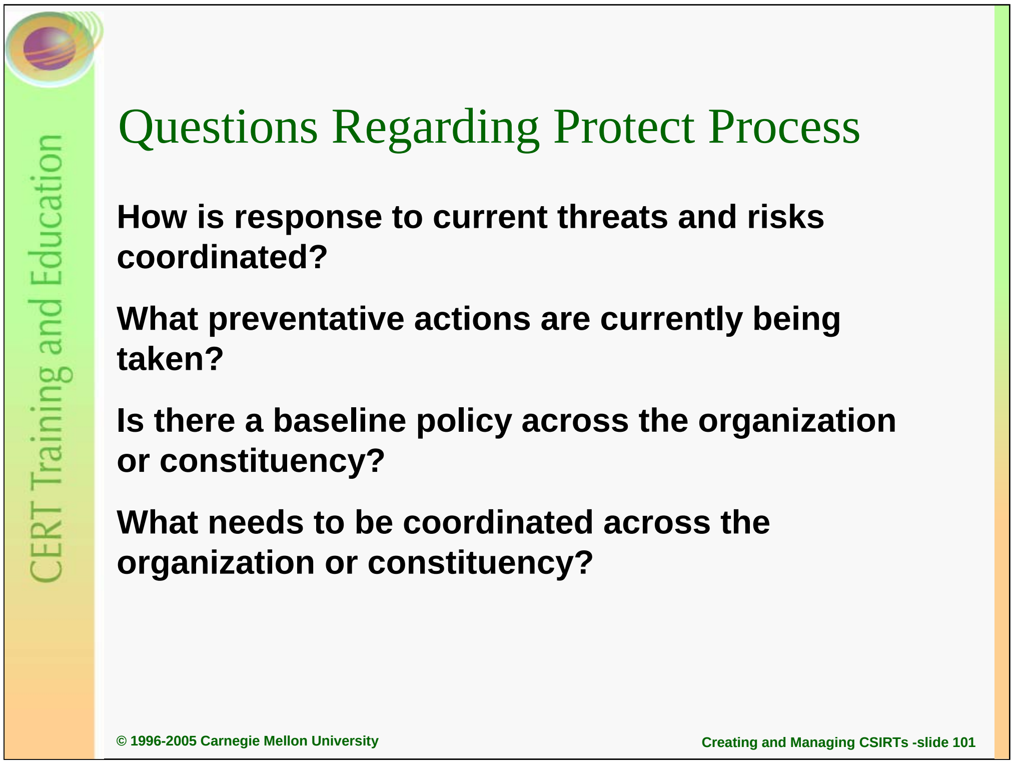
**Based on organizational mission and assigned job responsibilities for security and incident management, the protect subprocesses could be performed by a variety of personnel.**

**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.



CERT Training and Education

## Questions Regarding Protect Process

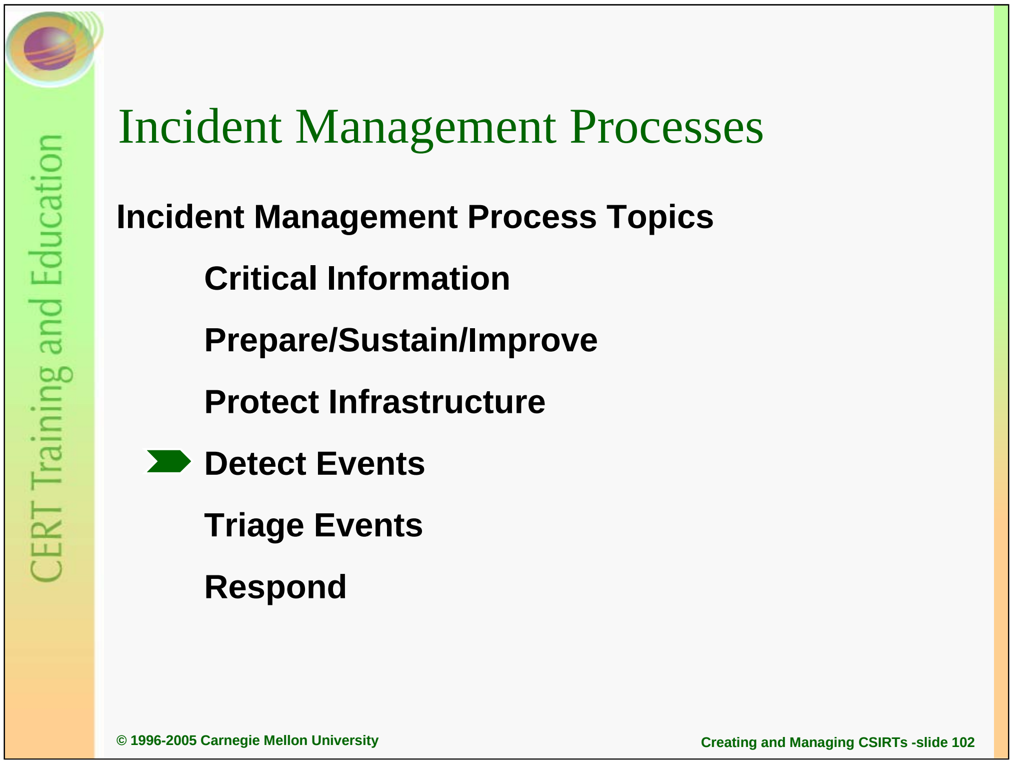
**How is response to current threats and risks coordinated?**

**What preventative actions are currently being taken?**

**Is there a baseline policy across the organization or constituency?**

**What needs to be coordinated across the organization or constituency?**

Creating and Managing CSIRTs -slide 101

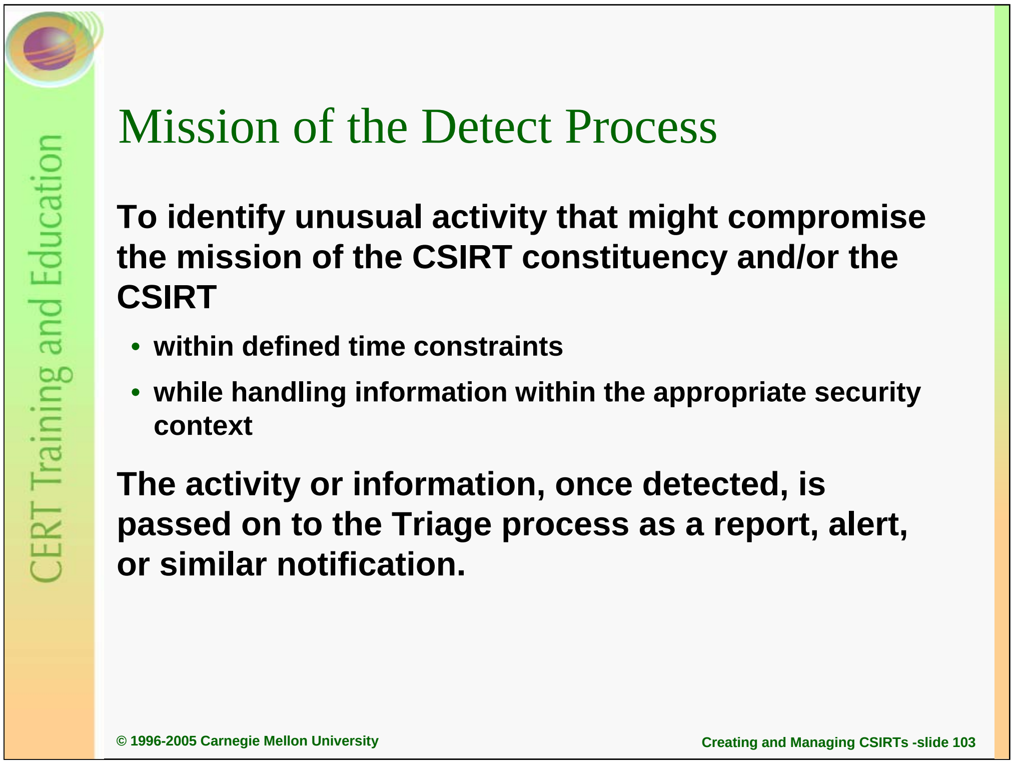


CERT Training and Education

# Incident Management Processes

**Incident Management Process Topics**

- **Critical Information**
- **Prepare/Sustain/Improve**
- **Protect Infrastructure**
- ➤ **Detect Events**
- **Triage Events**
- **Respond**



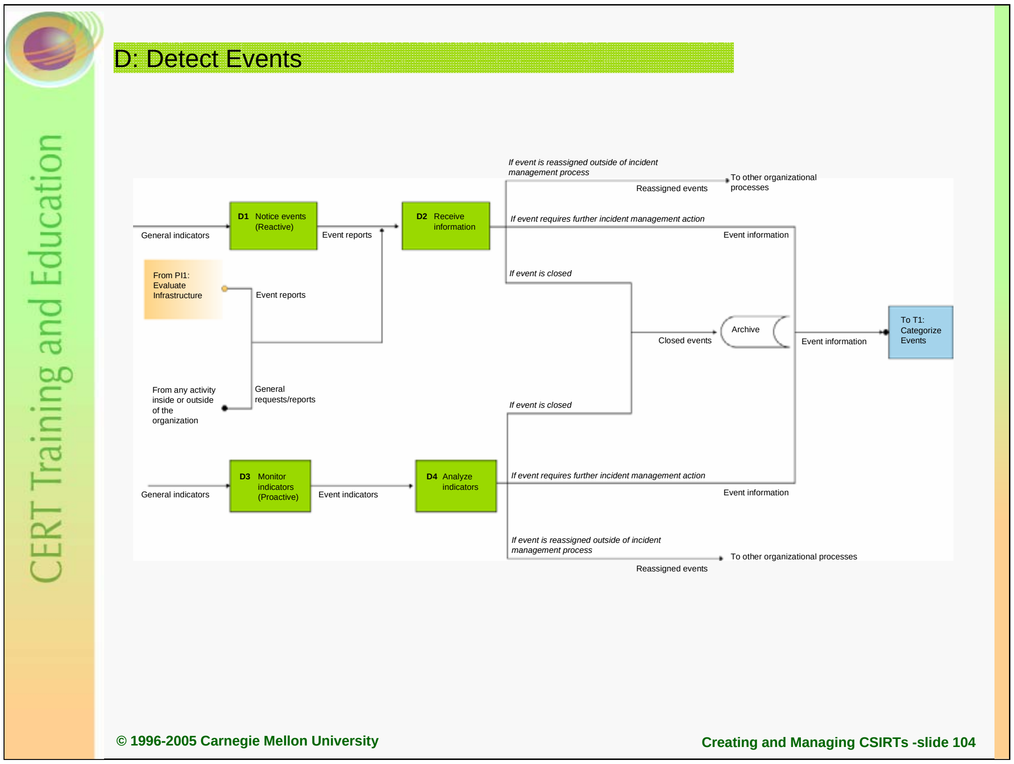
CERT Training and Education

# 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.**



CERT Training and Education

# D: Detect Events

General indicators

D1 Notice events (Reactive)

Event reports

D2 Receive information

From PI1: Evaluate Infrastructure

Event reports

From any activity inside or outside of the organization

General requests/reports

General indicators

D3 Monitor indicators (Proactive)

Event indicators

D4 Analyze indicators

*If event is reassigned outside of incident management process*

Reassigned events

To other organizational processes

*If event requires further incident management action*

Event information

*If event is closed*

Closed events

Archive

Event information

To T1: Categorize Events

*If event is closed*

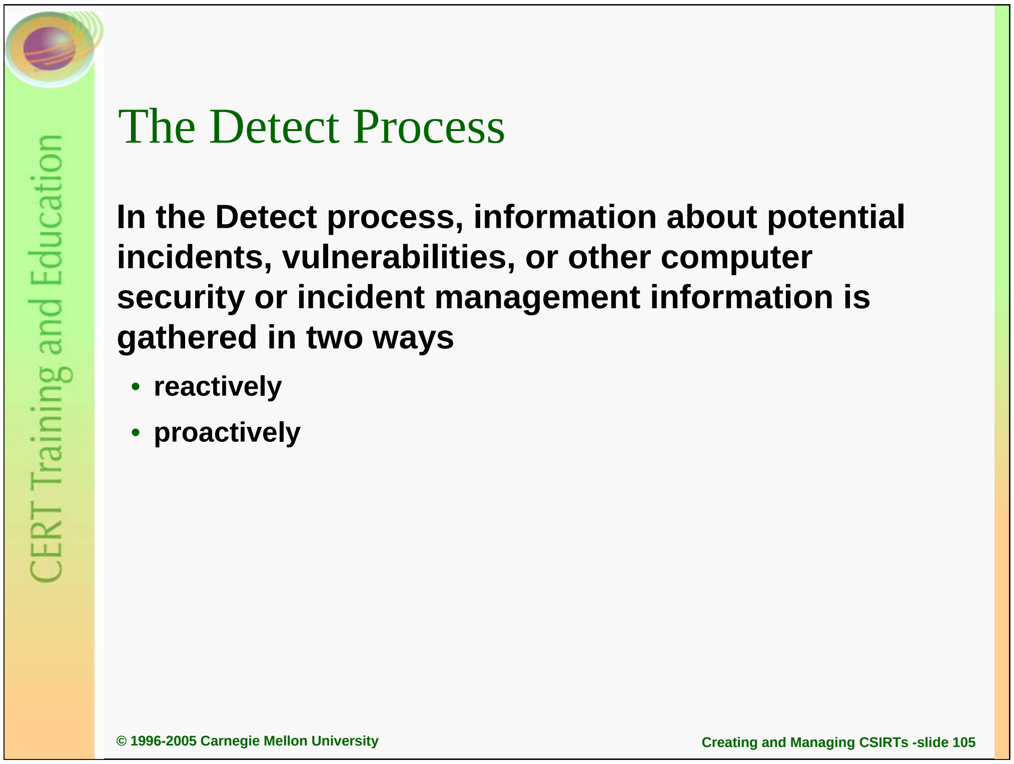
*If event requires further incident management action*

Event information

*If event is reassigned outside of incident management process*

To other organizational processes

Reassigned events



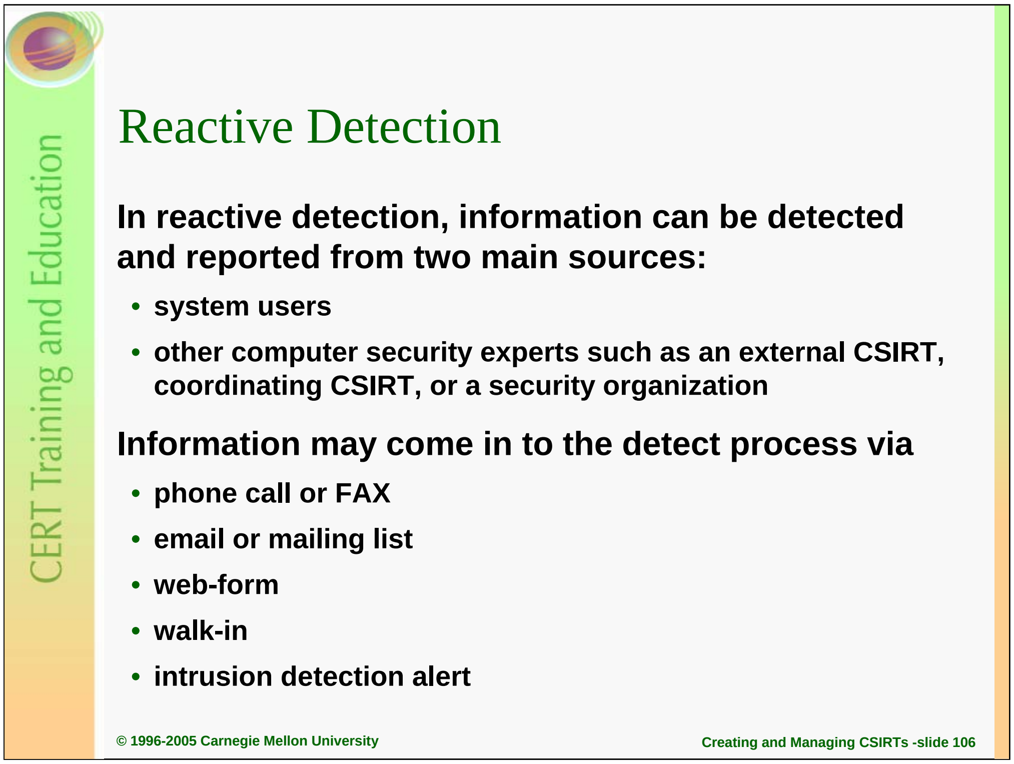
CERT Training and Education

# 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**

Creating and Managing CSIRTs -slide 105



CERT Training and Education

## 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**

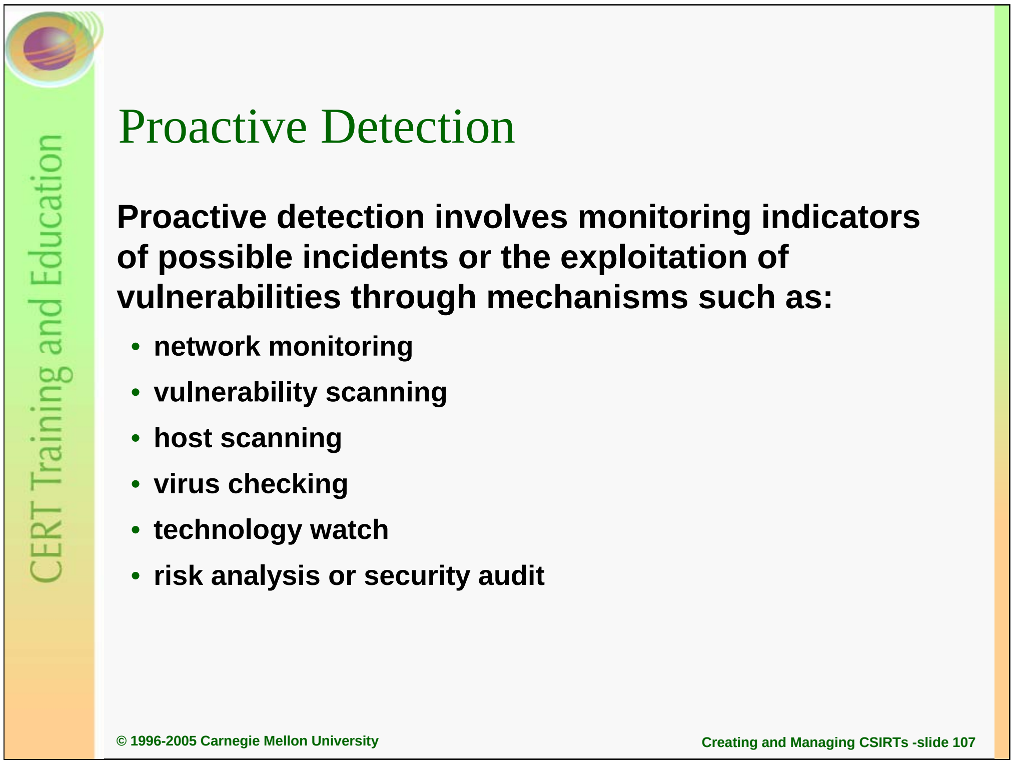
**Information may come in to the detect process via**

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

Creating and Managing CSIRTs -slide 106

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.



CERT Training and Education

## 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**
- **risk analysis or security audit**

© 1996-2005 Carnegie Mellon University

Creating and Managing CSIRTs -slide 107

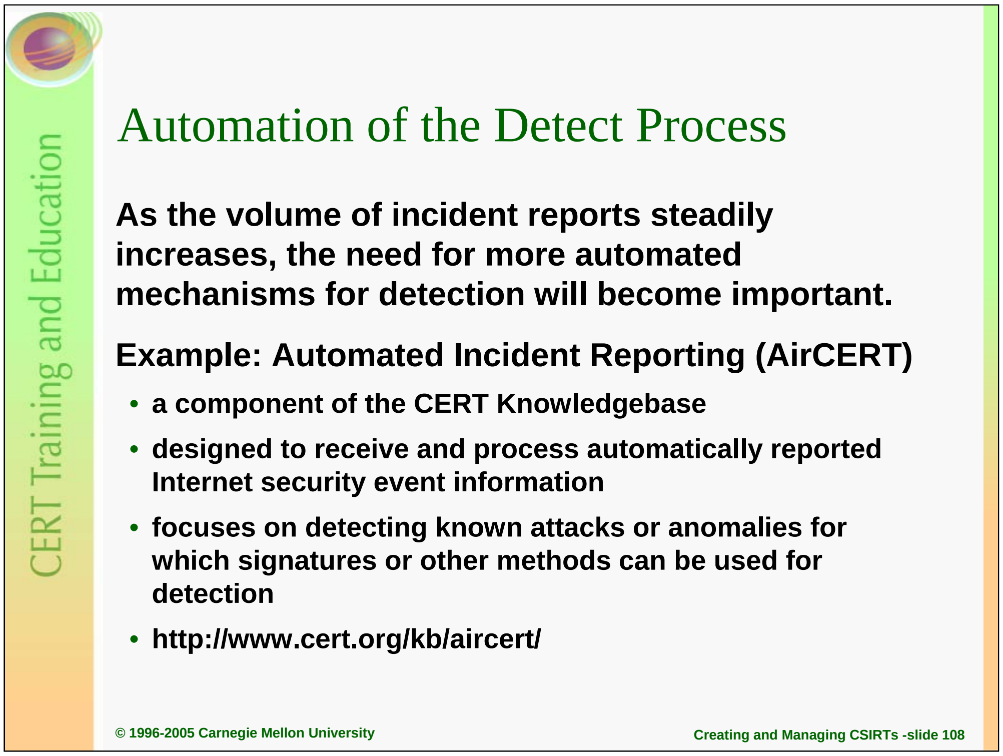
Proactive detection requires actions by the designated staff to identify suspicious activity. Staff proactively monitor a variety of data (such as host logs, firewall logs, and netflows) and use intrusion detection software to monitor network behavior, looking for indications of suspicious activity (D3).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

Staff performing such activity may be within or outside of a CSIRT function. Very often it is the IT 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 will have some criteria to follow to help them determine what type of alerts or suspicious activity should be passed on as a report to Triage. This occurs in process D4: Analyze Indicators, as shown in the D: Detect Events workflow diagram. 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



CERT Training and Education

## Automation of the Detect Process

**As the volume of incident reports steadily increases, the need for more automated mechanisms for detection will become important.**

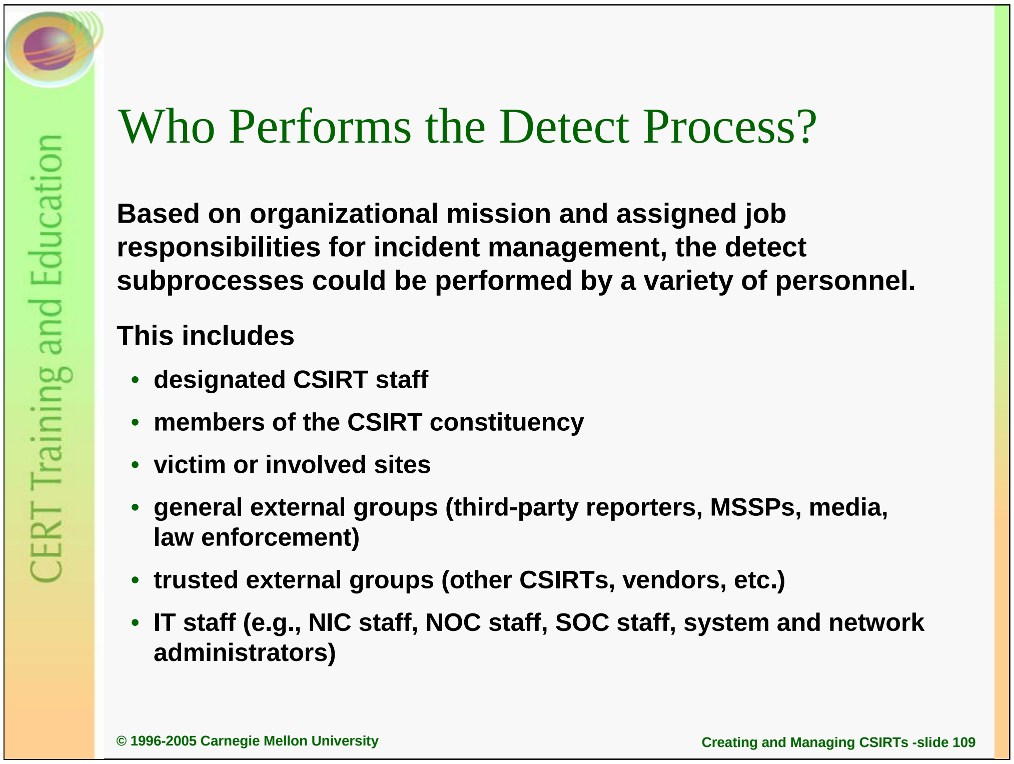
**Example: Automated Incident Reporting (AirCERT)**

- **a component of the CERT Knowledgebase**
- **designed to receive and process automatically reported Internet security event information**
- **focuses on detecting known attacks or anomalies for which signatures or other methods can be used for detection**
- **http://www.cert.org/kb/aircert/**

The CERT/CC has made available a prototype of a project called the Automated Incident Reporting, or “AirCERT”, that “involves the placement of Internet-based security event sensors on the networks of various organizations attached to the Internet. These sensors will log locally selected information on detected security events and anomalies to both a local database. If the site chooses, sanitized information can also be automatically sent to a central database located at the CERT/CC.

The CERT/CC is currently developing a prototype of this system using open source and low-cost components. The hope is to see this concept expanded so that various types of sensors from many vendors will be able to interoperate with the processes and databases developed for managing and analyzing security event information.”

http://www.cert.org/kb/aircert/



CERT Training and Education

## 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.**

**This includes**

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

Personnel for noticing and reporting events can include

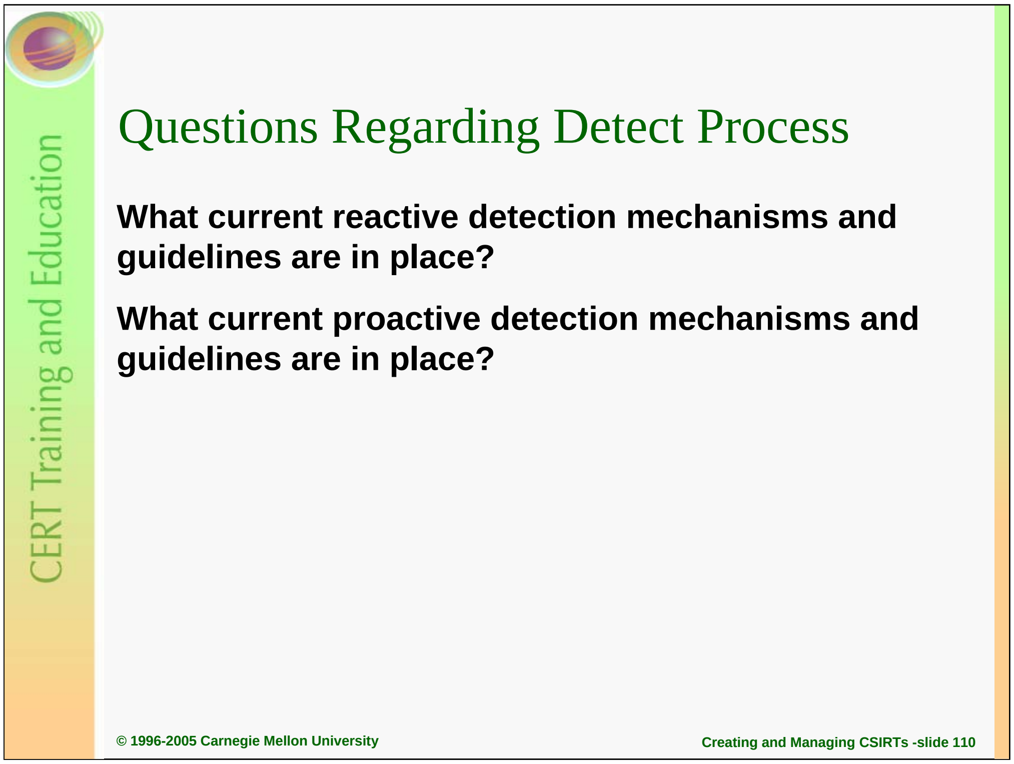
- CSIRT
- CSIRT constituency
- victim or involved sites
- general external groups (third-party reporters, MSSPs, media, law enforcement)
- trusted external groups (other CSIRTs, vendors, etc.)
- IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators)
- coordination center

Personnel for receiving reported information can 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 staff, NOC staff, system and network administrators)
- selected members of the CSIRT staff
- third parties (e.g., regulatory bodies, MSSPs, collaborators, ISPs, trusted SMEs)
- coordination center

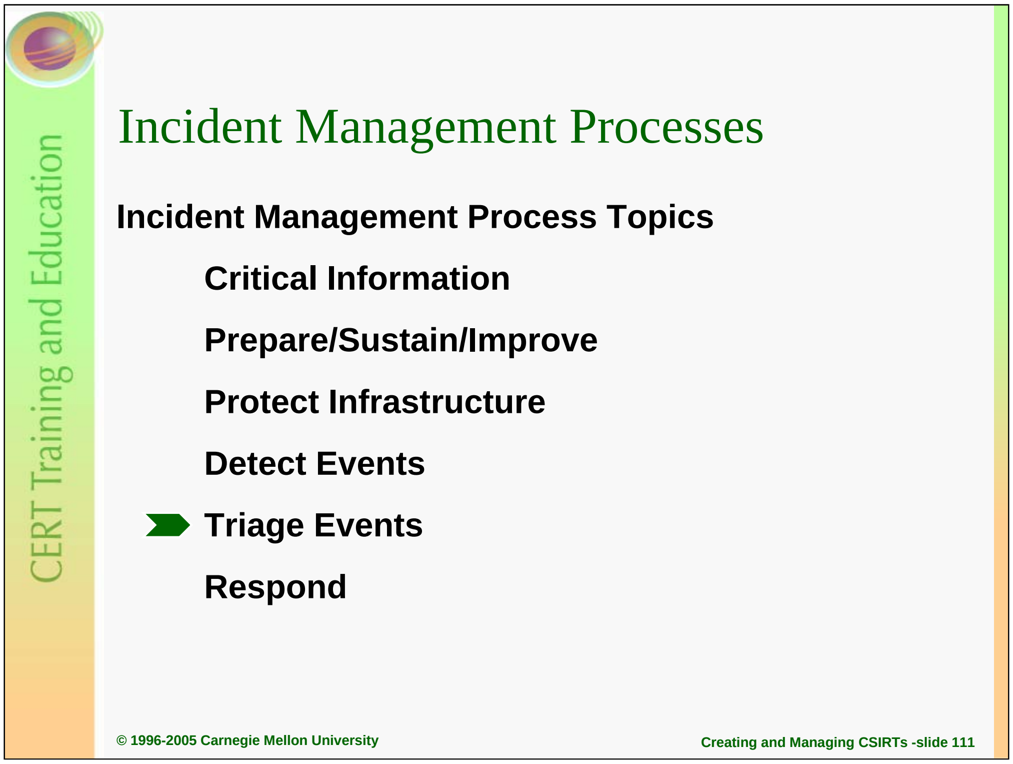


CERT Training and Education

# Questions Regarding Detect Process

What current reactive detection mechanisms and guidelines are in place?

What current proactive detection mechanisms and guidelines are in place?

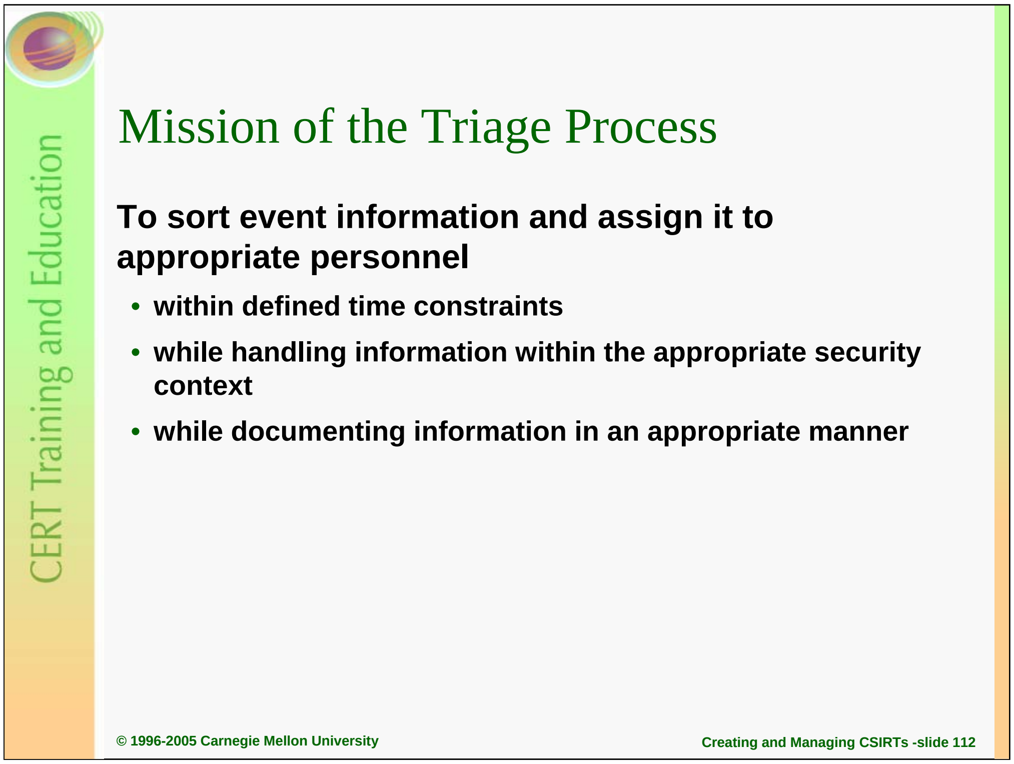


CERT Training and Education

# Incident Management Processes

**Incident Management Process Topics**

- **Critical Information**
- **Prepare/Sustain/Improve**
- **Protect Infrastructure**
- **Detect Events**
- ➤ **Triage Events**
- **Respond**



CERT Training and Education

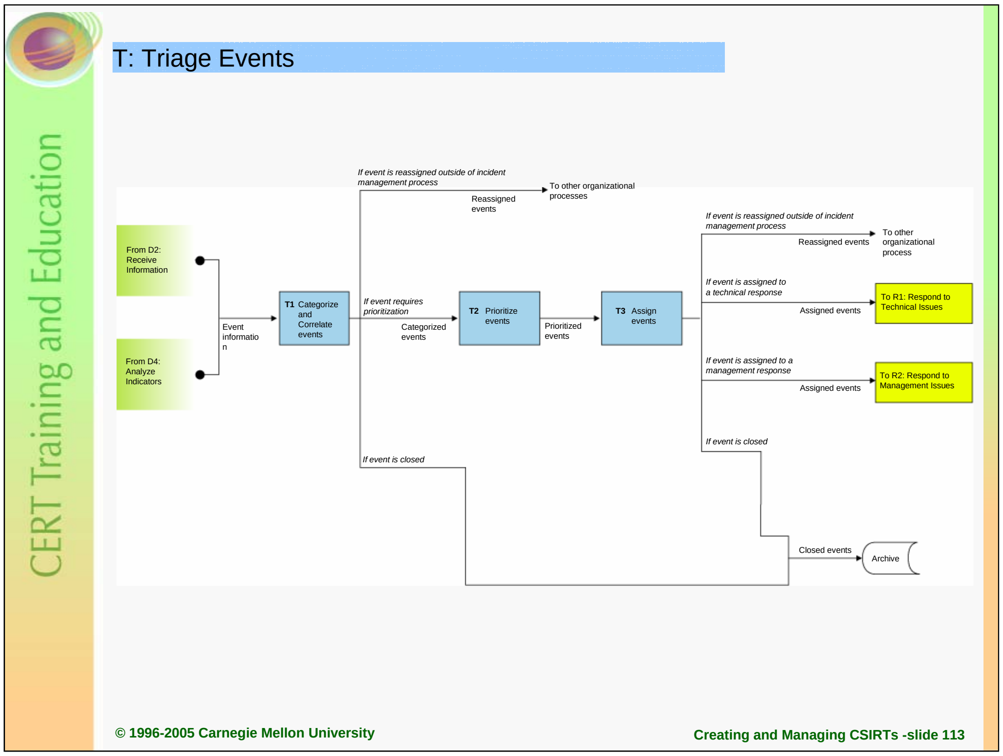
# Mission of the Triage Process

**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**

Creating and Managing CSIRTs -slide 112

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.



CERT Training and Education

## T: Triage Events

From D2: Receive Information

From D4: Analyze Indicators

Event informatio n

**T1** Categorize and Correlate events

*If event is reassigned outside of incident management process*

Reassigned events

To other organizational processes

*If event requires prioritization*

Categorized events

**T2** Prioritize events

Prioritized events

**T3** Assign events

*If event is reassigned outside of incident management process*

Reassigned events

To other organizational process

*If event is assigned to a technical response*

Assigned events

To R1: Respond to Technical Issues

*If event is assigned to a management response*

Assigned events

To R2: Respond to Management Issues

*If event is closed*

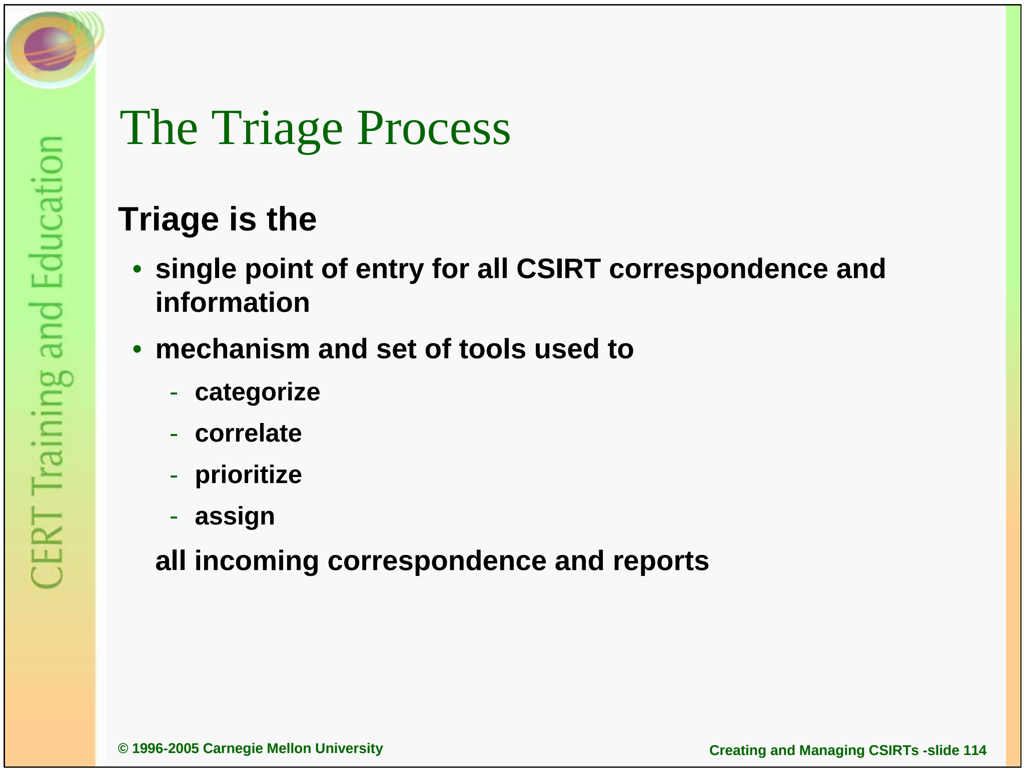
*If event is closed*

Closed events

Archive

Creating and Managing CSIRTs -slide 113

Triage is the process of sorting, categorizing, correlating, prioritizing, and assigning 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.



CERT Training and Education

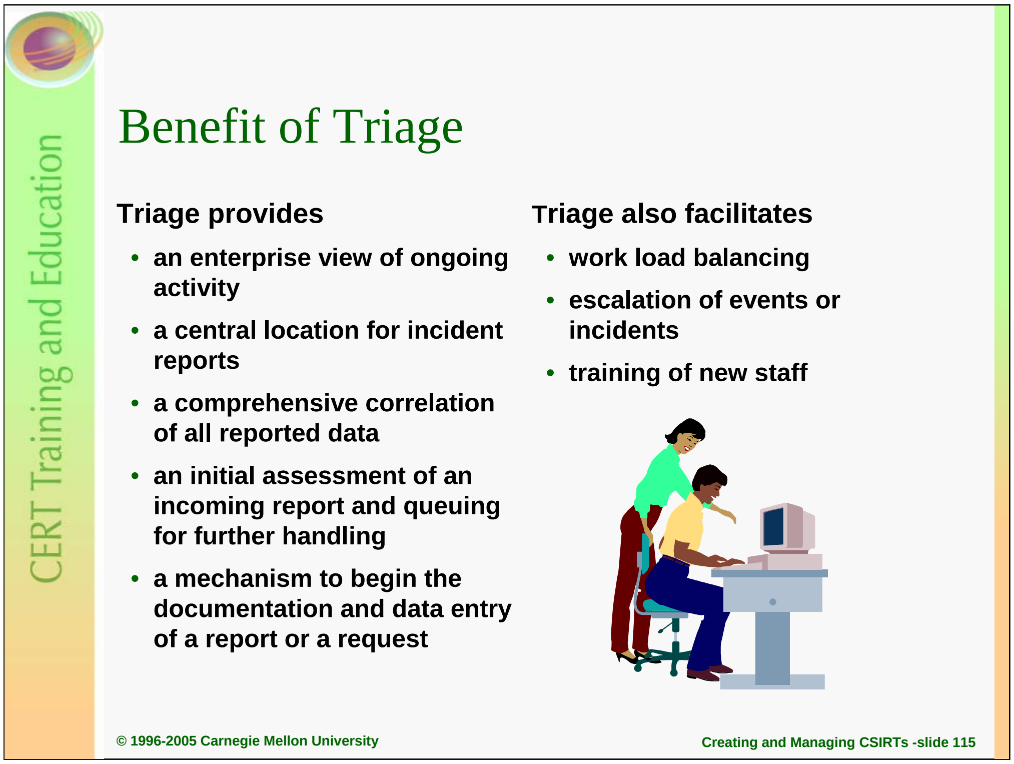
## The Triage Process

**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.



CERT Training and Education

## Benefit 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

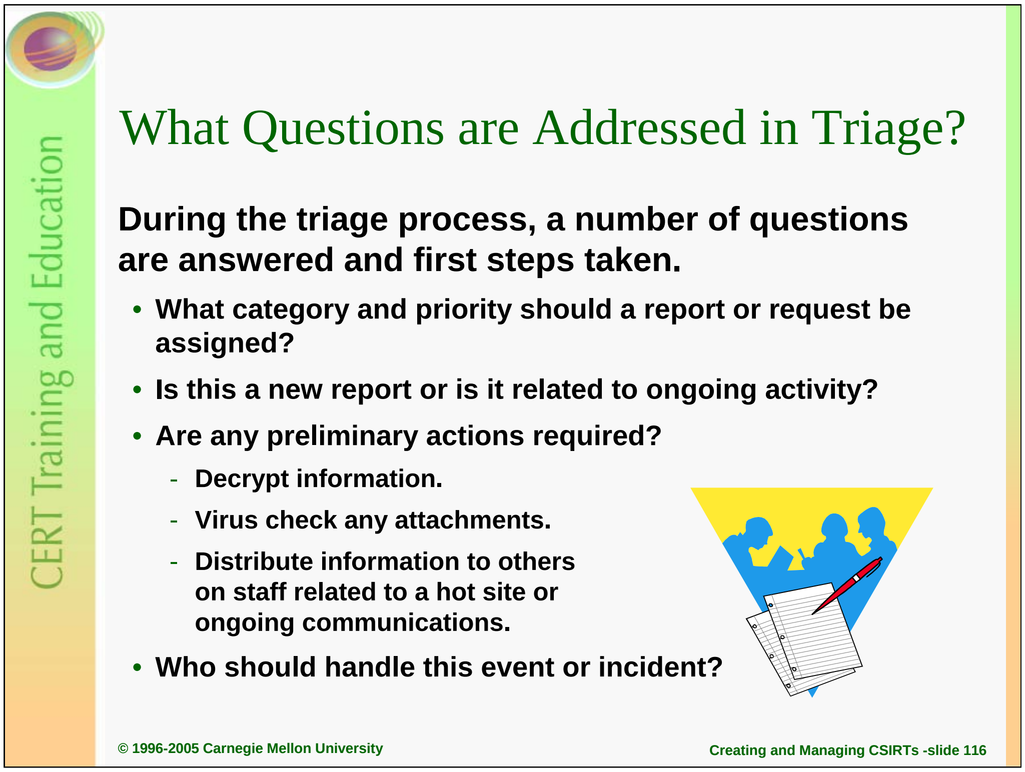
Creating and Managing CSIRTs -slide 115

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



CERT Training and Education

## 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?**

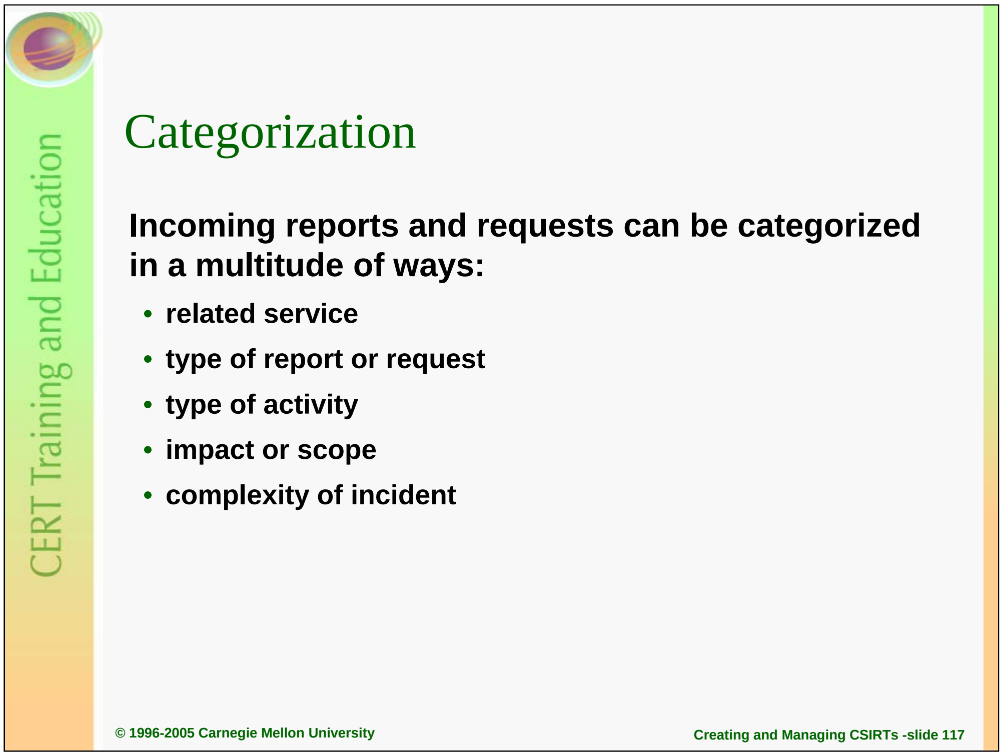
Creating and Managing CSIRTs -slide 116

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”.



CERT Training and Education

# Categorization

**Incoming reports and requests can be categorized in a multitude of ways:**

- **related service**
- **type of report or request**
- **type of activity**
- **impact or scope**
- **complexity of incident**

© 1996-2005 Carnegie Mellon University

Creating and Managing CSIRTs -slide 117

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)

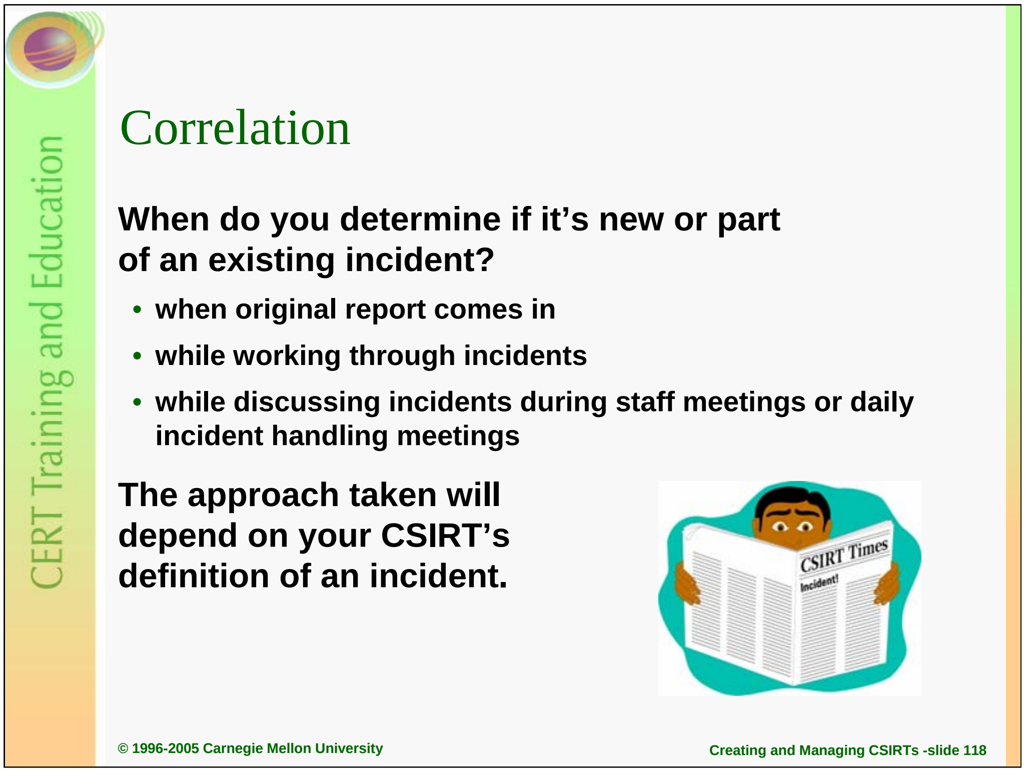
- unknown
- user compromise
- root compromise
- misuse of resources
- denial of service
- reconn
- deception
- false alarm
- virus
- information request
- vulnerability report
- hoax

The National Institute of Science and Technology lists the following categories of incidents in their publication: *Computer Security Incident Handling Guide, National Institute of Standards and Technology (NIST SP 800-61)* :

- denial of service
- malicious code
- unauthorized access
- inappropriate usage
- multiple component

Rand Europe's *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries* lists the following categories:

- computer fingerprinting
- malicious code
- denial of service
- account compromise
- intrusion attempt
- unauthorized access to information
- unauthorized access to transmissions
- unauthorized modification of information
- unauthorized access to communications systems



CERT Training and Education

## Correlation

**When do you determine if it’s new or part of an existing incident?**

- **when original report comes in**
- **while working through incidents**
- **while discussing incidents during staff meetings or daily incident handling meetings**

**The approach taken will depend on your CSIRT’s definition of an incident.**

CSIRT Times
Incident!

Correlation is looking at how many reports relate to one particular incident; this can help determine the scope and severity of the activity.

Determination is based on

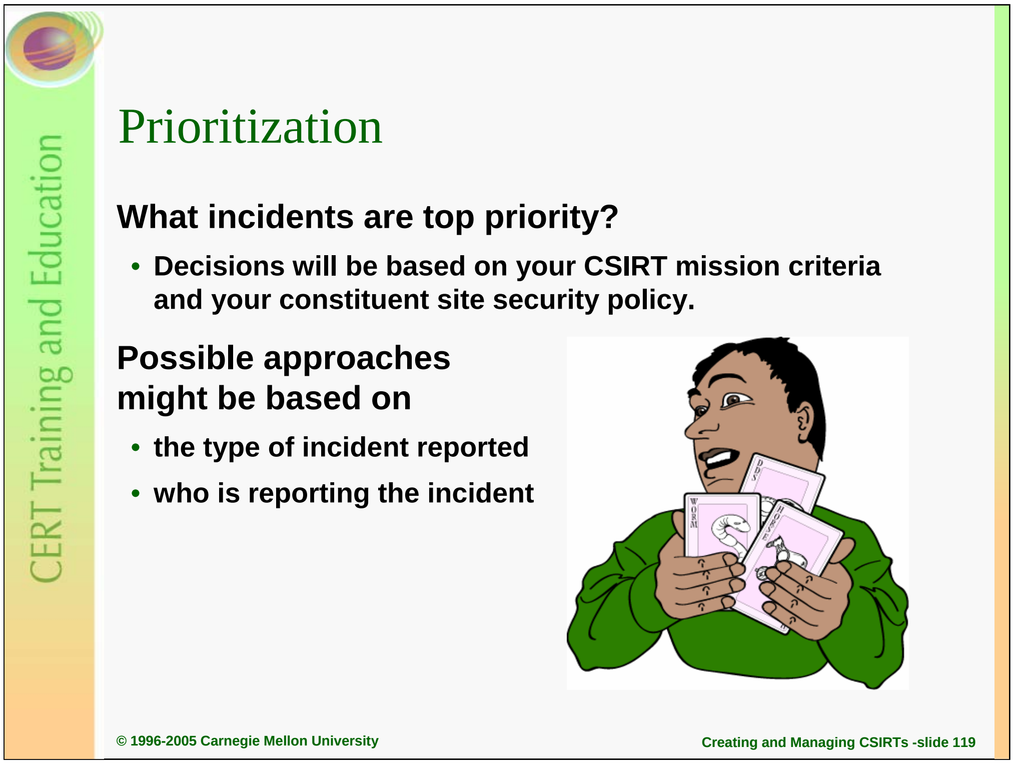
- hosts involved
- activity/attack method used
- timing of “attacks”
- reference number(s)

Separately tracked incidents could be recognized as part of the same activity.

Your CSIRT procedures should define how to track or merge such incidents.

- Who will follow up?
- What reference number(s) will be used?

The classification of a request or event can involve not only determining what type of event is being reported (e.g., a denial of service, a privileged compromise, or reconnaissance activity) but also a correlation with other events and incidents. For example, is this a new report or is this report part of an ongoing incident? Is it a known attack type or is it some new intruder methodology? If an event is determined to be part of an ongoing incident, its priority and assignment may be automatically set to be the same as that incident. In this case the correlation actually impacts and affects the categorization, priority, and assignment of the event. Because of this relationship, these processes can occur in parallel.



CERT Training and Education

## Prioritization

**What incidents are top priority?**

- **Decisions will be based on your CSIRT mission criteria and your constituent site security policy.**

**Possible approaches might be based on**

- **the type of incident reported**
- **who is reporting the incident**

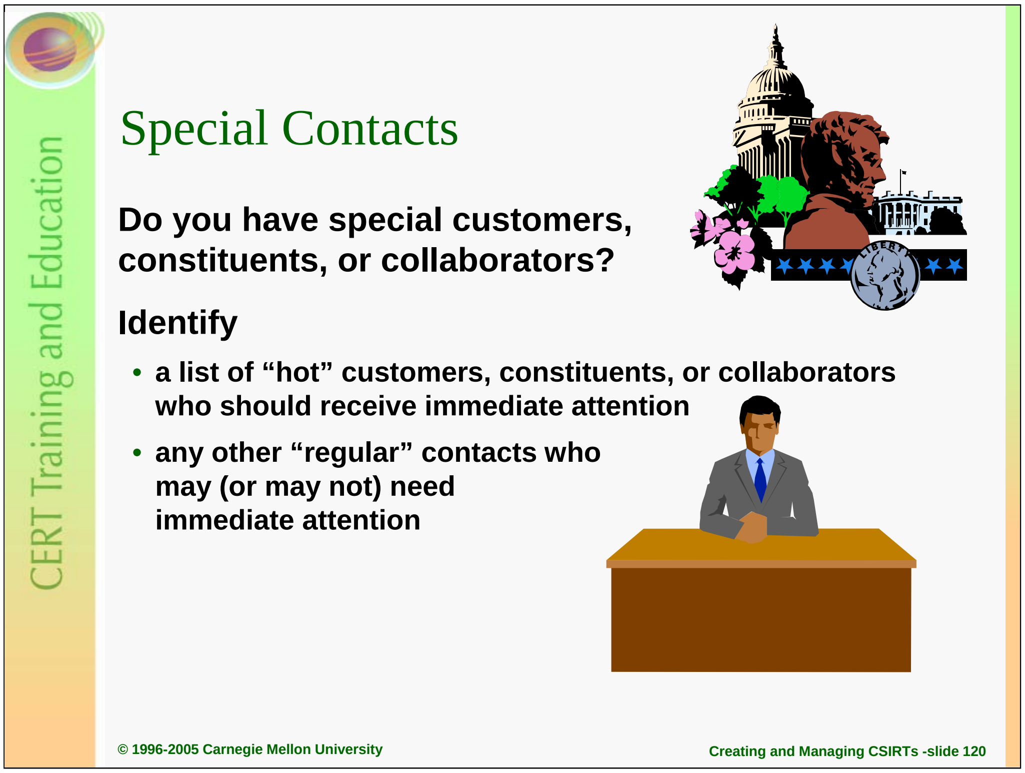
Creating and Managing CSIRTs -slide 119

If the event is not part of an ongoing incident, then after it is categorized, it is passed to the Prioritize process (T2). Certain categories of events may actually have their own predefined priorities, so again, the T1, T2, and T3 processes (as outlined in the workflow diagram) may occur at the same time or as part of the same process. Even if there is not an assigned priority to the category, these two processes may occur so fast that they seem to be part of the same process. Other times it may take additional analysis to determine the priority.

Decision criteria might involve

- protecting sensitive information
- limiting financial loss
- maintaining infrastructure integrity
- danger to human life
- threat to CSIRT systems
- threat to Internet infrastructure
- type of activity
- scope of activity
- relationship to other ongoing security related and non-security related activity

In the SEI Technical Report CMU/SEI-2003-TR-001, *The State of the Practice of CSIRTs*, a review of various priority and severity criteria in various incident management related books was performed. Table 12 of that document, *Methods of Categorizing and Prioritizing Incident Reports and Activity*, shows the results of that review.



CERT Training and Education

## Special Contacts

**Do you have special customers, constituents, or collaborators?**

**Identify**

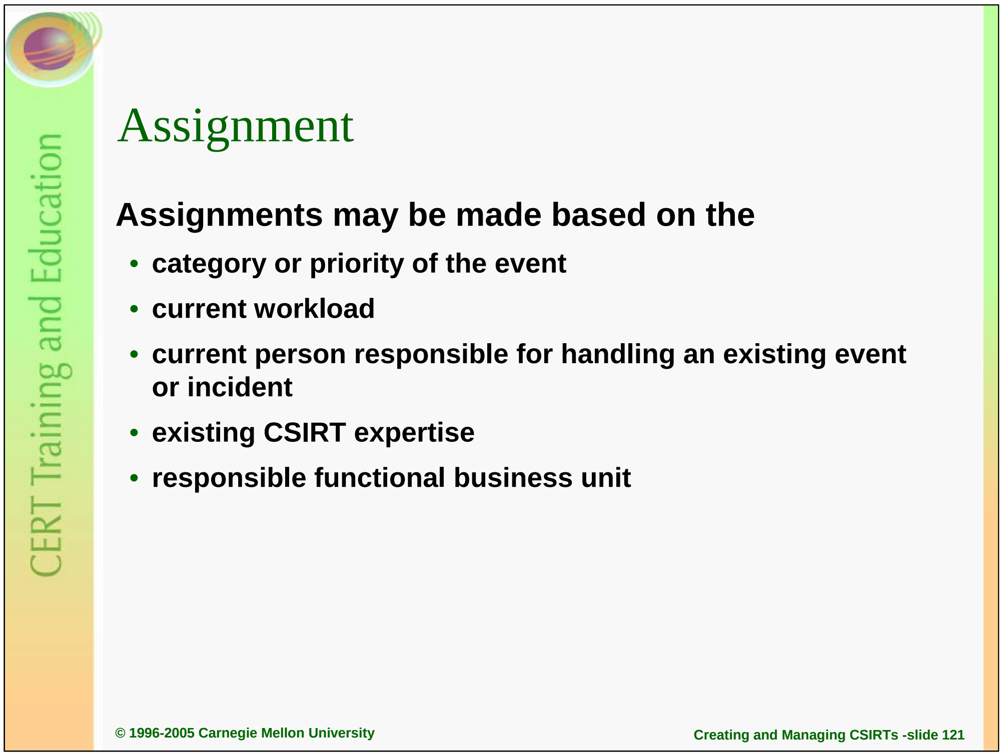
- **a list of “hot” customers, constituents, or collaborators who should receive immediate attention**
- **any other “regular” contacts who may (or may not) need immediate attention**

Creating and Managing CSIRTs -slide 120

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.



CERT Training and Education

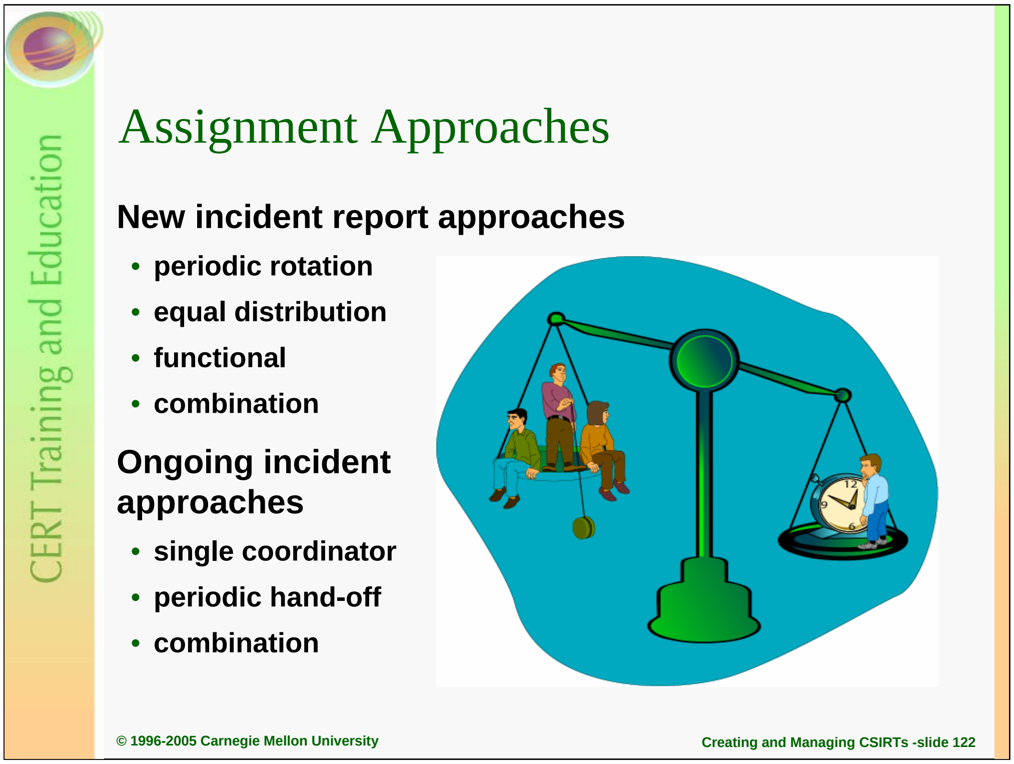
## Assignment

**Assignments may be made based on the**

- **category or priority of the event**
- **current workload**
- **current person responsible for handling an existing event or incident**
- **existing CSIRT expertise**
- **responsible functional business unit**

Creating and Managing CSIRTs -slide 121

If information is notable or suspicious, it is assigned to someone in the Respond process and passed on to that process. It should be noted that the categorization and priority, as well as the assignment, might be changed when the event is analyzed in the Respond process.



CERT Training and Education

## Assignment Approaches

**New incident report approaches**

- **periodic rotation**
- **equal distribution**
- **functional**
- **combination**

**Ongoing incident approaches**

- **single coordinator**
- **periodic hand-off**
- **combination**

Creating and Managing CSIRTs -slide 122

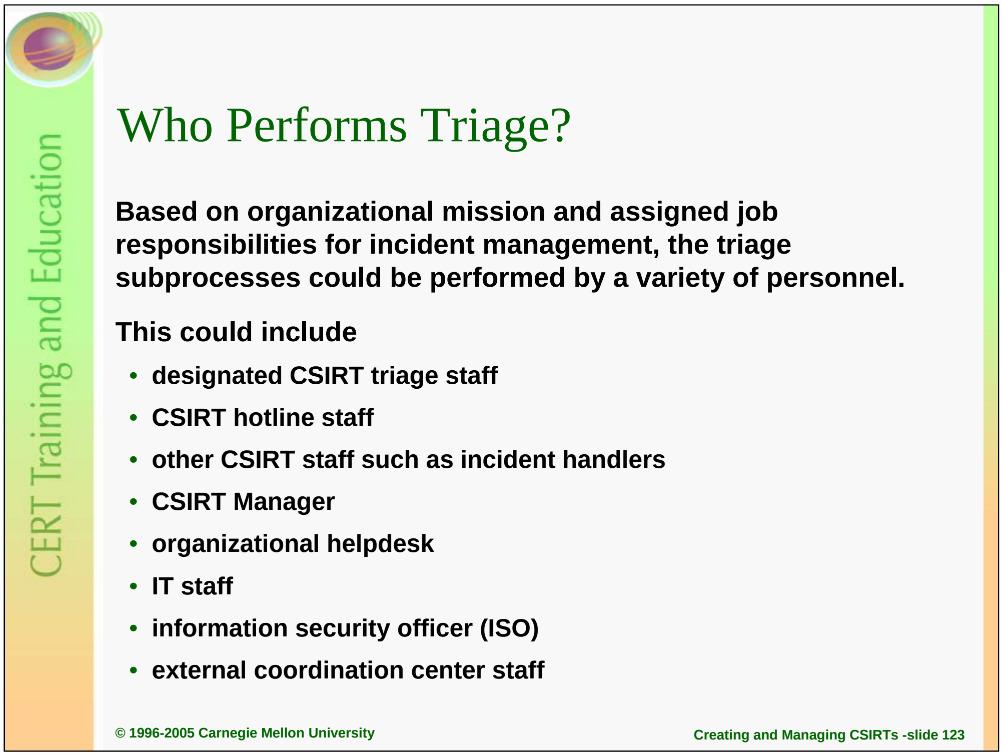
How does your team “balance” the workload?

New incident report approaches

- periodic rotation
  - All new incidents are assigned to a designated incident handler; the assignee changes at designated intervals.
- equal distribution
  - All new reports are reviewed and distributed equally among available incident handlers.
- functional
  - All new reports are reviewed and those reports in areas where a designated incident handler has particular expertise are given to that person; viruses, Windows, Linux, etc. are examples of functional areas of expertise.
- combination
  - After-hours reports are periodically rotated; new reports during working hours are equally distributed.

Ongoing incident approaches

- single incident handler
  - Each incident is handled by one staff member from initial report until closure.
- periodic hand-off
  - Open incidents are handed off to a new lead person at designated intervals.
- combination
  - Incidents are given to a single, lead incident handler but can be handed off when necessary.



CERT Training and Education

# 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.**

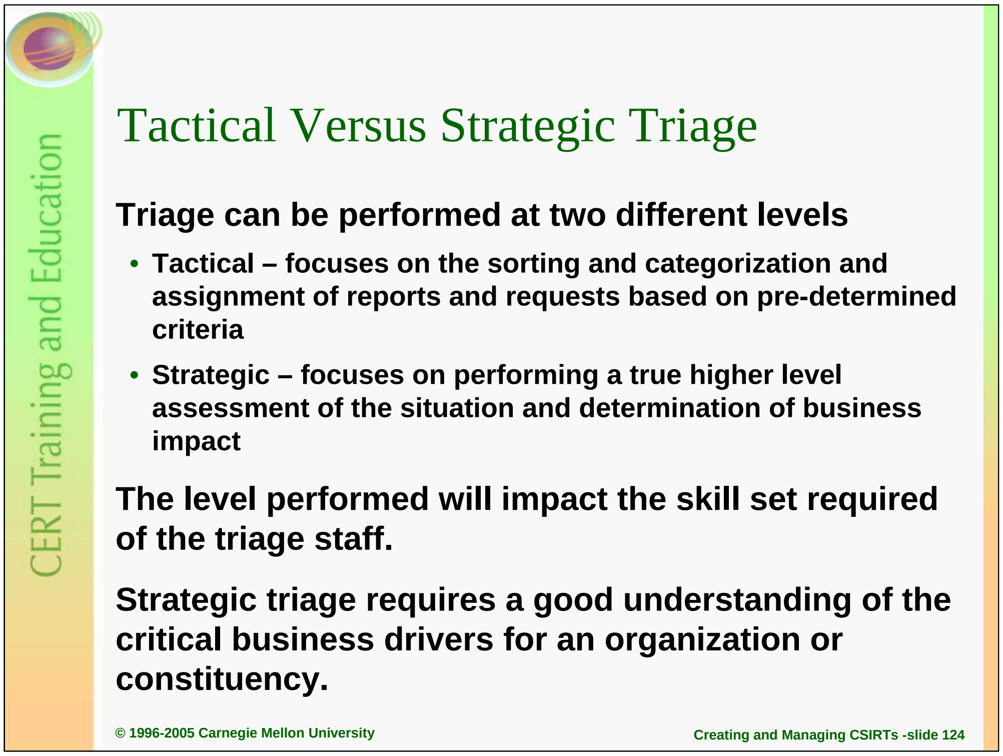
**This could include**

- **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**

Creating and Managing CSIRTs -slide 123

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.



CERT Training and Education

## 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**

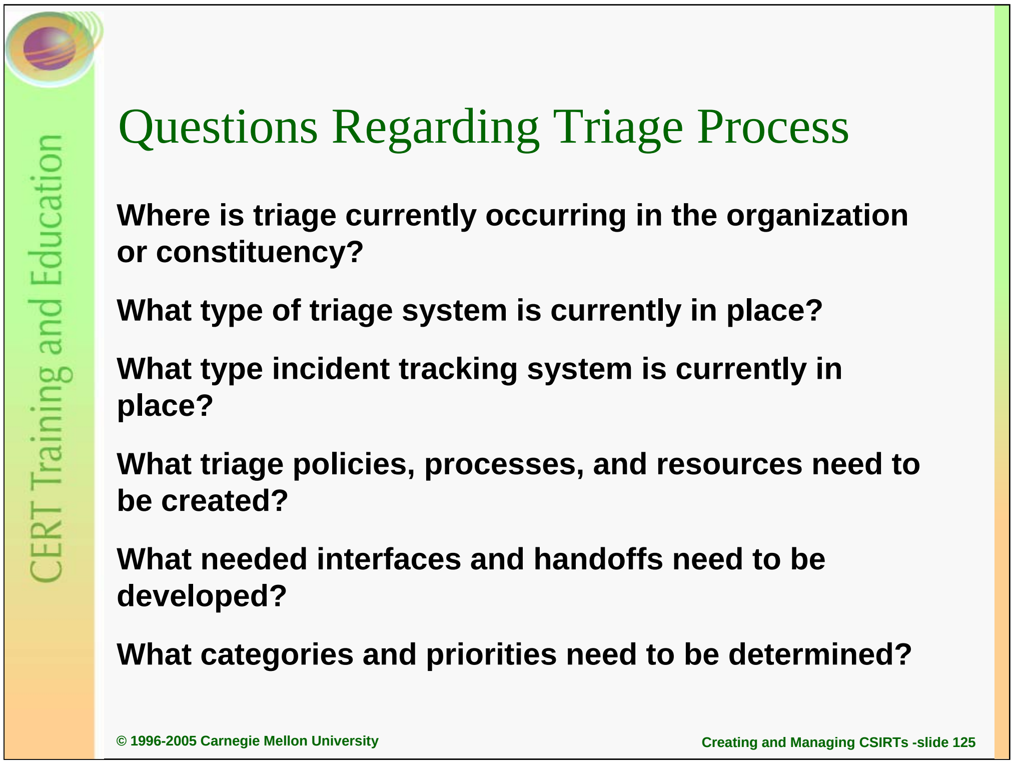
**The level performed will impact the skill set required of the triage staff.**

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

Creating and Managing CSIRTs -slide 124

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.



CERT Training and Education

## Questions Regarding Triage Process

Where is triage currently occurring in the organization or constituency?

What type of triage system is currently in place?

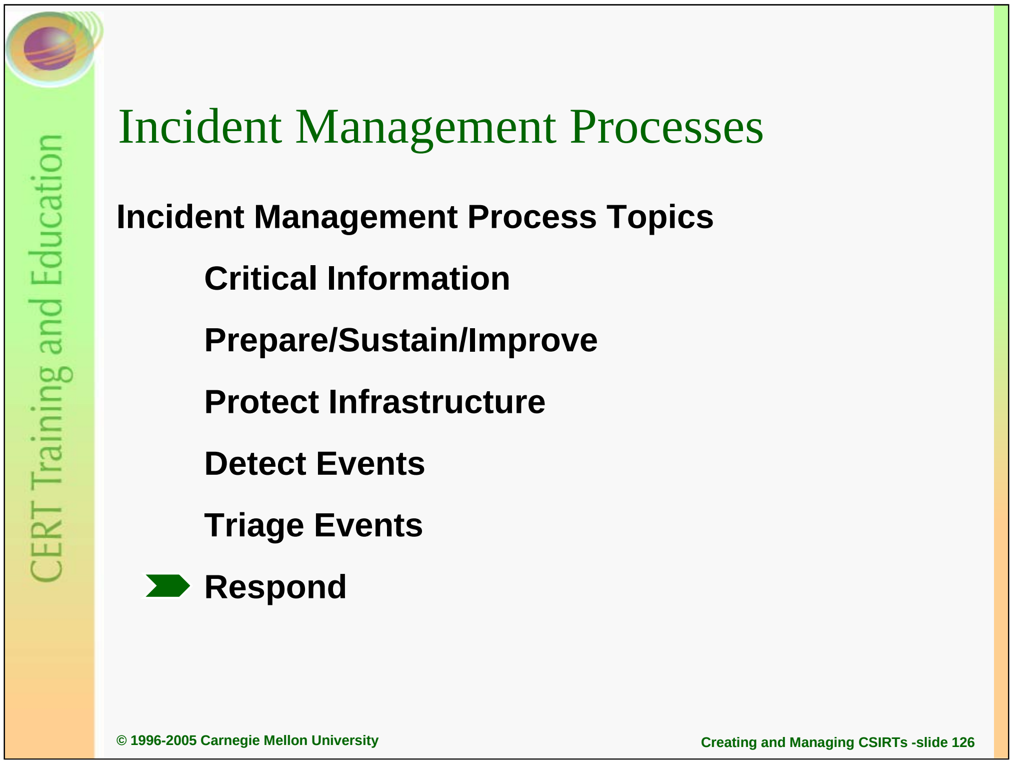
What type incident tracking system is currently in place?

What triage policies, processes, and resources need to be created?

What needed interfaces and handoffs need to be developed?

What categories and priorities need to be determined?

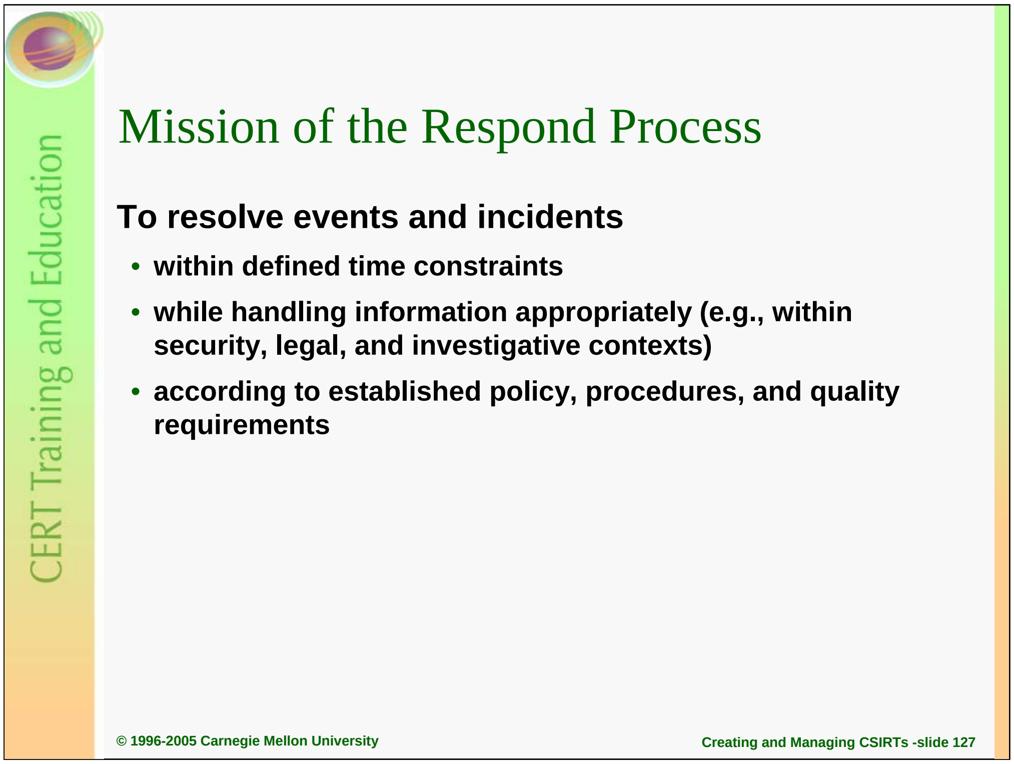
Creating and Managing CSIRTs -slide 125


CERT Training and Education

## Incident Management Processes

**Incident Management Process Topics**

- **Critical Information**
- **Prepare/Sustain/Improve**
- **Protect Infrastructure**
- **Detect Events**
- **Triage Events**
- ➤ **Respond**

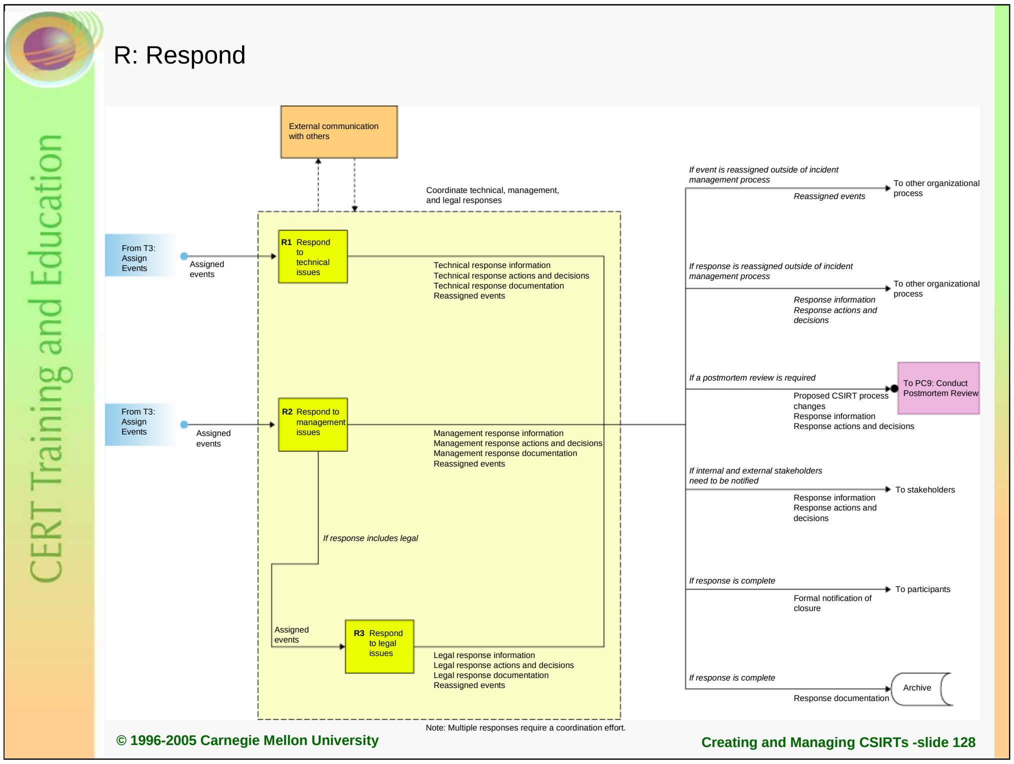


CERT Training and Education

# 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**



CERT Training and Education

R: Respond

External communication with others

Coordinate technical, management, and legal responses

From T3: Assign Events

Assigned events

R1 Respond to technical issues

Technical response information
Technical response actions and decisions
Technical response documentation
Reassigned events

From T3: Assign Events

Assigned events

R2 Respond to management issues

Management response information
Management response actions and decisions
Management response documentation
Reassigned events

*If response includes legal*

Assigned events

R3 Respond to legal issues

Legal response information
Legal response actions and decisions
Legal response documentation
Reassigned events

*If event is reassigned outside of incident management process*

*Reassigned events*

To other organizational process

*If response is reassigned outside of incident management process*

*Response information*
*Response actions and decisions*

To other organizational process

*If a postmortem review is required*

Proposed CSIRT process changes
Response information
Response actions and decisions

To PC9: Conduct Postmortem Review

*If internal and external stakeholders need to be notified*

Response information
Response actions and decisions

To stakeholders

*If response is complete*

Formal notification of closure

To participants

*If response is complete*

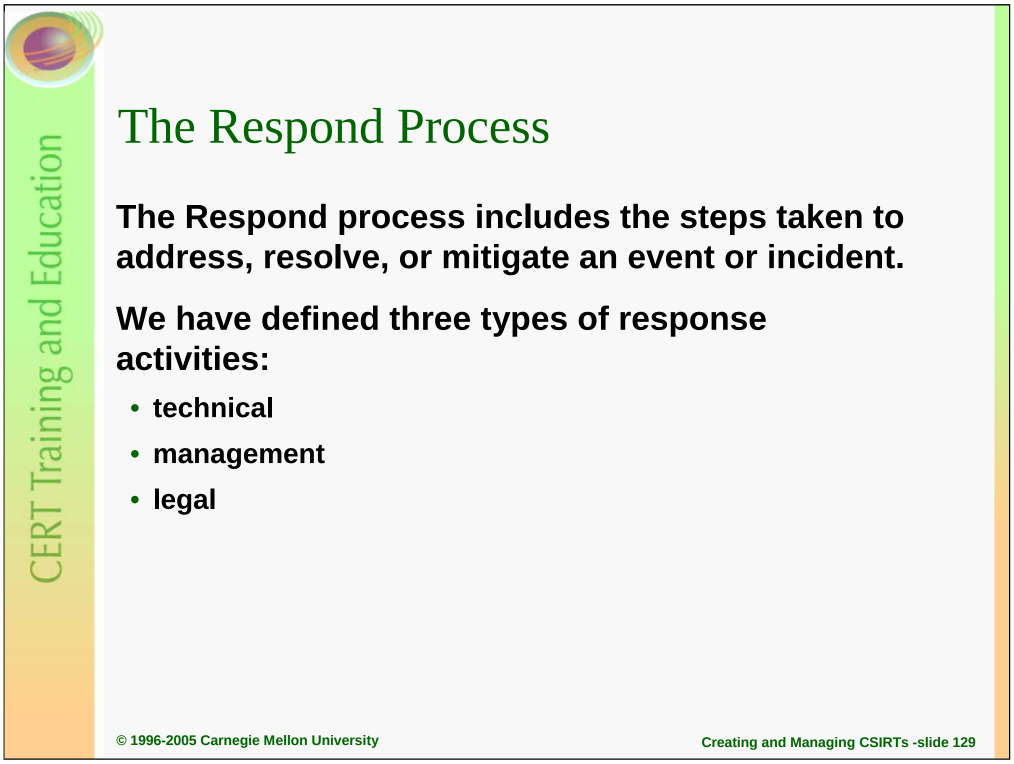
Response documentation

Archive

Note: Multiple responses require a coordination effort.

Creating and Managing CSIRTs -slide 128

Coordination should occur across all three areas of the Respond process for the process to be efficient and effective. This means that all those involved in the response must communicate the steps that are being taken and any relevant information. It also means that during a particular type of response (a technical response, for example), a need may be seen to get management or legal staff involved. This type of cooperation and coordination should occur through established channels of communication that should be outlined in the 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. Sometimes all three processes will be initiated to resolve an incident, and sometimes only one or two of the processes will be required. However many are activated, some type of leader or project coordinator for the Respond process is needed to ensure that all the appropriate tasks are being performed across all the response actors.



CERT Training and Education

## The Respond Process

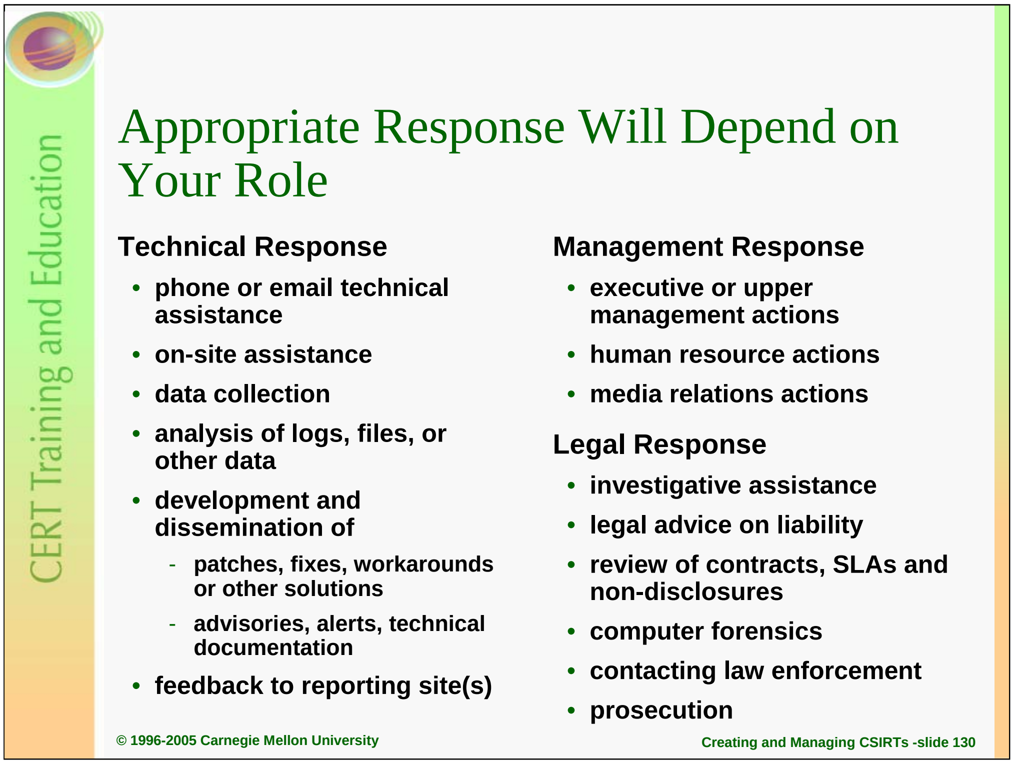
**The Respond process includes the steps taken to address, resolve, or mitigate an event or incident.**

**We have defined three types of response activities:**

- **technical**
- **management**
- **legal**

Creating and Managing CSIRTs -slide 129

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.



# Appropriate Response Will Depend 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

Creating and Managing CSIRTs -slide 130

Each CSIRT provides a response

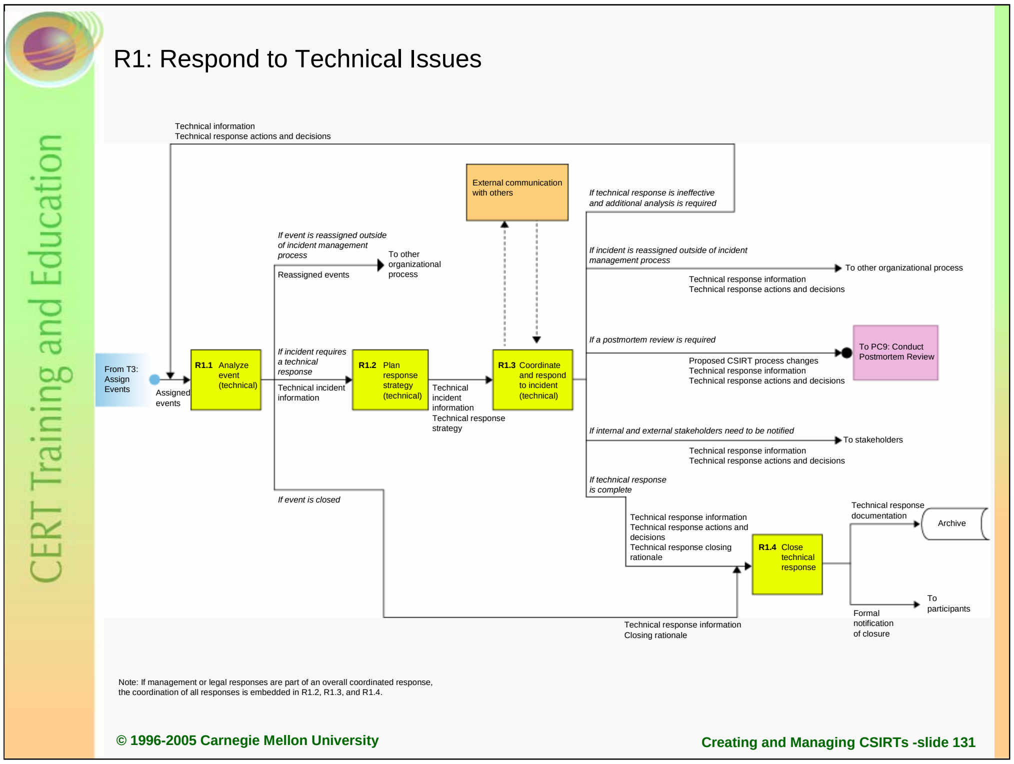
- defined by the CSIRT mission and goals
- guided by the CSIRT policy and procedures
- in conjunction with other parts of the organization according to their roles and responsibilities

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.



## R1: Respond to Technical Issues

CERT Training and Education
Technical information
Technical response actions and decisions
External communication with others
If technical response is ineffective and additional analysis is required
If event is reassigned outside of incident management process
To other organizational process
Reassigned events
If incident is reassigned outside of incident management process
To other organizational process
Technical response information
Technical response actions and decisions
If a postmortem review is required
To PC9: Conduct Postmortem Review
Proposed CSIRT process changes
Technical response information
Technical response actions and decisions
From T3: Assign Events
Assigned events
R1.1 Analyze event (technical)
If incident requires a technical response
Technical incident information
R1.2 Plan response strategy (technical)
Technical incident information
Technical response strategy
R1.3 Coordinate and respond to incident (technical)
If internal and external stakeholders need to be notified
To stakeholders
Technical response information
Technical response actions and decisions
If technical response is complete
If event is closed
Technical response information
Technical response actions and decisions
Technical response closing rationale
R1.4 Close technical response
Technical response documentation
Archive
To participants
Formal notification of closure
Technical response information
Closing rationale

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.

Creating and Managing CSIRTs -slide 131

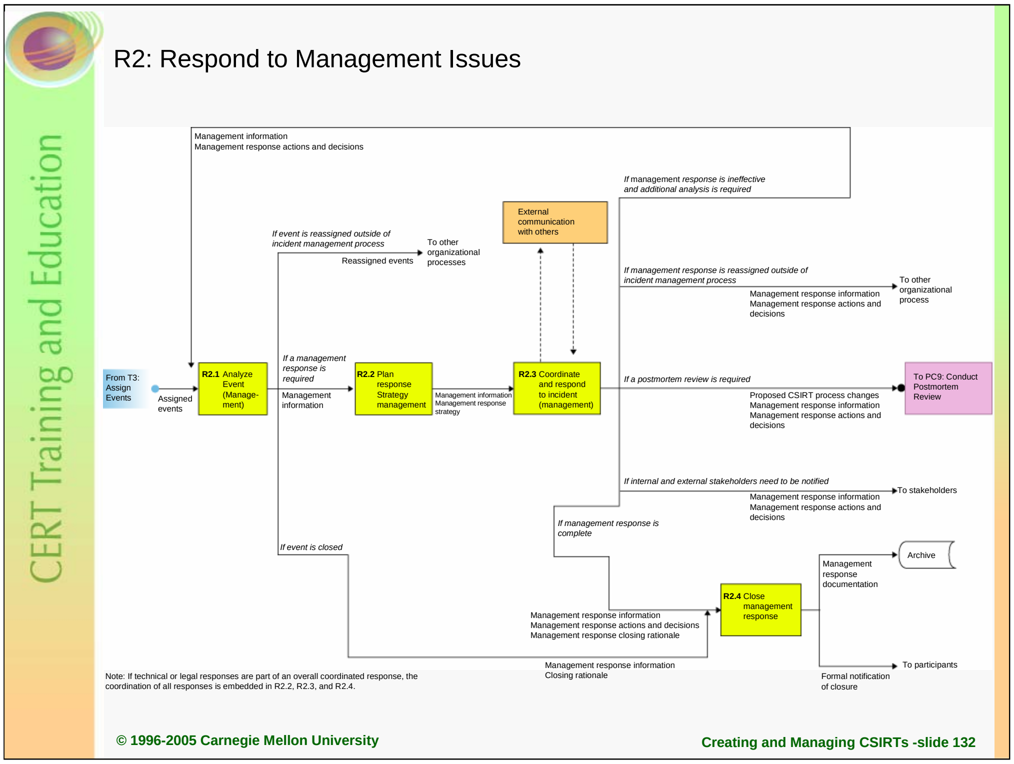
In this subprocess workflow, the response focuses on the actions taken by the technical staff to analyze and resolve an event or incident. Technical staff can include CSIRT staff such as incident, artifact, and vulnerability handlers, as well as other technical staff internal and external to the organization, 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

- whom 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.



CERT Training and Education

## R2: Respond to Management Issues

Management information
Management response actions and decisions
If management response is ineffective and additional analysis is required
External communication with others
If event is reassigned outside of incident management process
Reassigned events
To other organizational processes
If management response is reassigned outside of incident management process
Management response information
Management response actions and decisions
To other organizational process
From T3: Assign Events
Assigned events
R2.1 Analyze Event (Manage-ment)
If a management response is required
Management information
R2.2 Plan response Strategy management
Management information
Management response strategy
R2.3 Coordinate and respond to incident (management)
If a postmortem review is required
Proposed CSIRT process changes
Management response information
Management response actions and decisions
To PC9: Conduct Postmortem Review
If internal and external stakeholders need to be notified
To stakeholders
Management response information
Management response actions and decisions
If management response is complete
If event is closed
Management response information
Management response actions and decisions
Management response closing rationale
R2.4 Close management response
Management response documentation
Archive
Management response information
Closing rationale
To participants
Formal notification of closure

Note: If technical or legal responses are part of an overall coordinated response, the coordination of all responses is embedded in R2.2, R2.3, and R2.4.

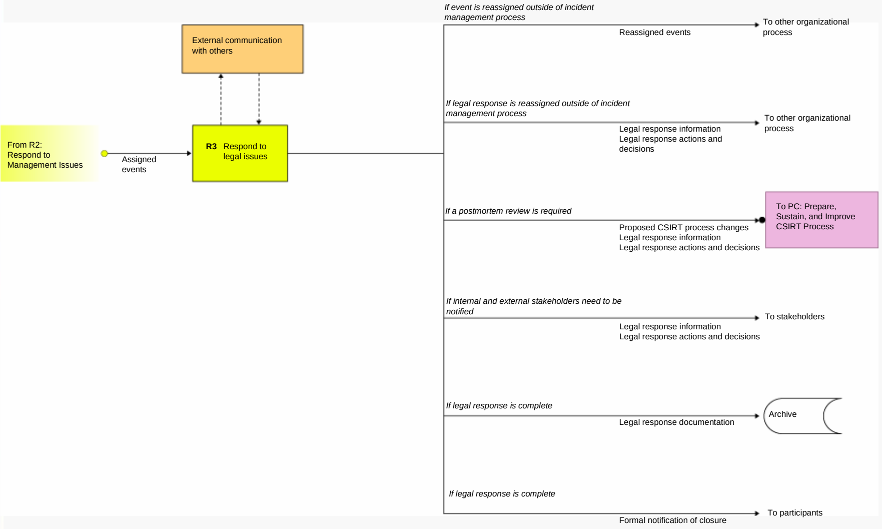
Creating and Managing CSIRTs -slide 132

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).

CERT Training and Education

## R3: Respond to Legal Issues



From R2: Respond to Management Issues

Assigned events

**R3** Respond to legal issues

External communication with others

*If event is reassigned outside of incident management process*

Reassigned events

To other organizational process

*If legal response is reassigned outside of incident management process*

Legal response information
Legal response actions and decisions

To other organizational process

*If a postmortem review is required*

Proposed CSIRT process changes
Legal response information
Legal response actions and decisions

To PC: Prepare, Sustain, and Improve CSIRT Process

*If internal and external stakeholders need to be notified*

Legal response information
Legal response actions and decisions

To stakeholders

*If legal response is complete*

Legal response documentation

Archive

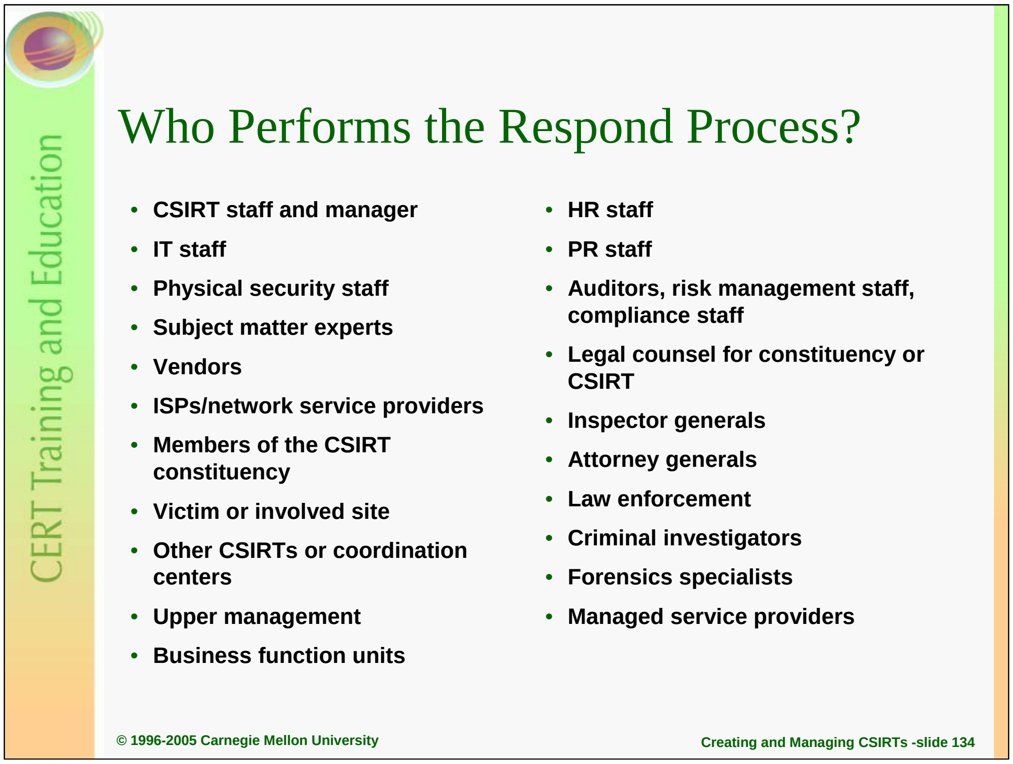
*If legal response is complete*

Formal notification of closure

To participants

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.

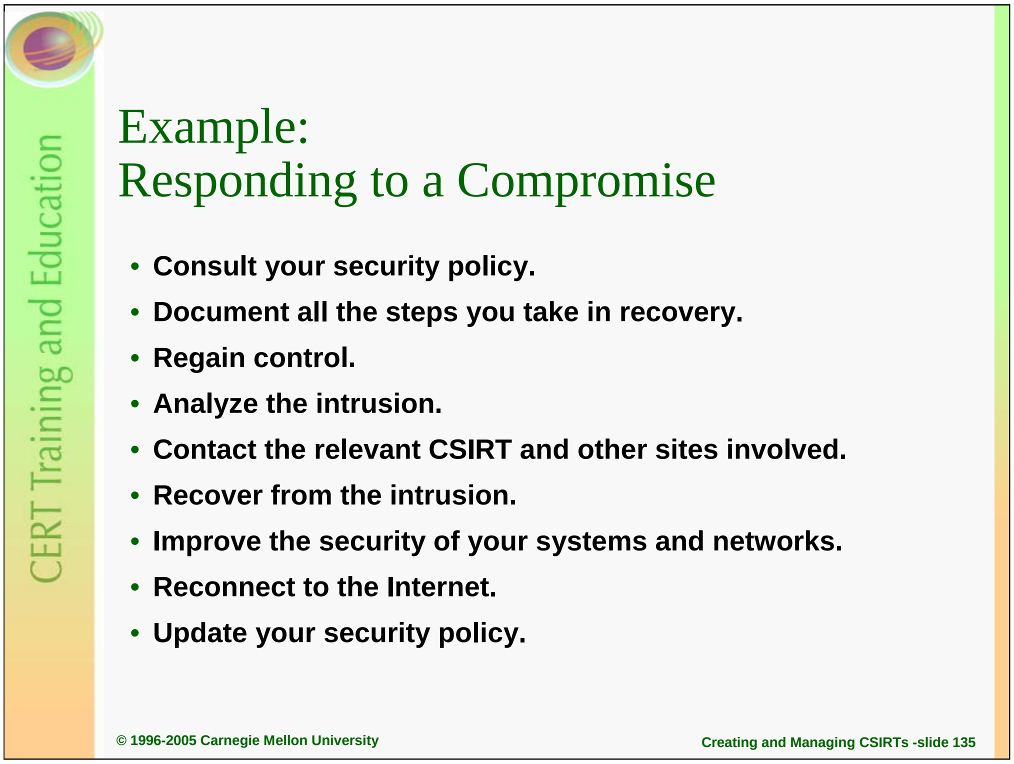

CERT Training and Education

## Who Performs the Respond Process?

- CSIRT staff and manager
- IT staff
- Physical security staff
- Subject matter experts
- Vendors
- ISPs/network service providers
- Members of the CSIRT constituency
- Victim or involved site
- 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

Creating and Managing CSIRTs -slide 134

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

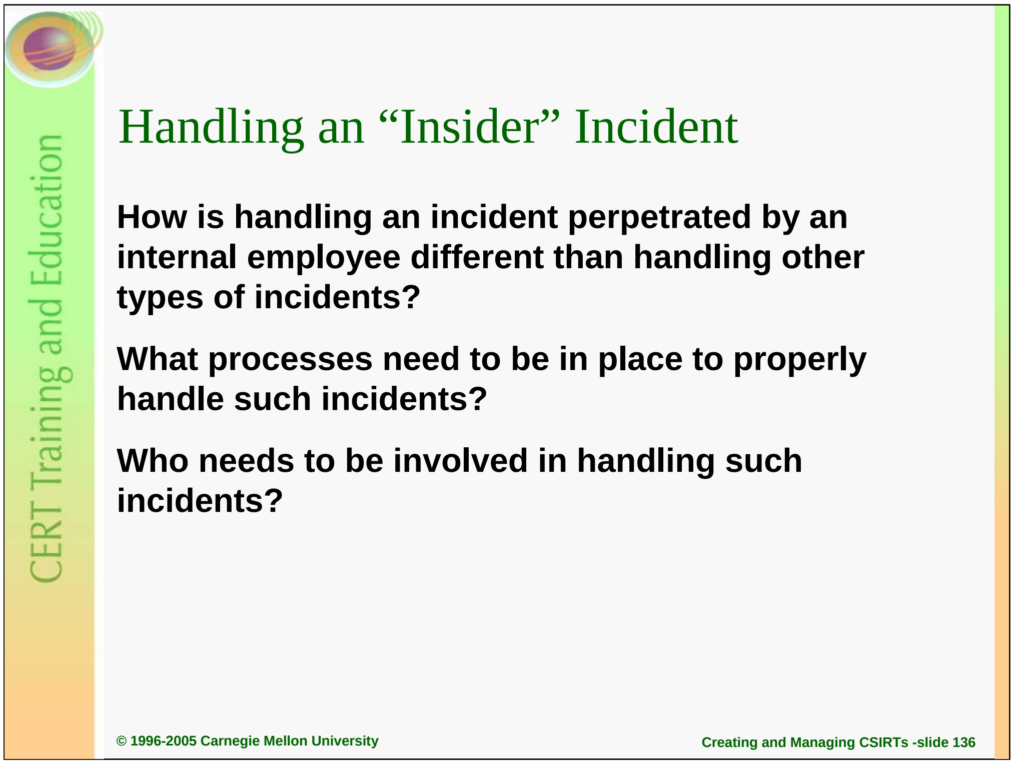


CERT Training and Education

## Example:<br>Responding to a Compromise

- Consult your security policy.
- Document all the steps you take in recovery.
- Regain control.
- Analyze the intrusion.
- Contact the relevant CSIRT and other sites involved.
- Recover from the intrusion.
- Improve the security of your systems and networks.
- Reconnect to the Internet.
- Update your security policy.

Creating and Managing CSIRTs -slide 135


CERT Training and Education

## Handling an "Insider" Incident

**How is handling an incident perpetrated by an internal employee different than handling other types of incidents?**

**What processes need to be in place to properly handle such incidents?**

**Who needs to be involved in handling such incidents?**

Creating and Managing CSIRTs -slide 136

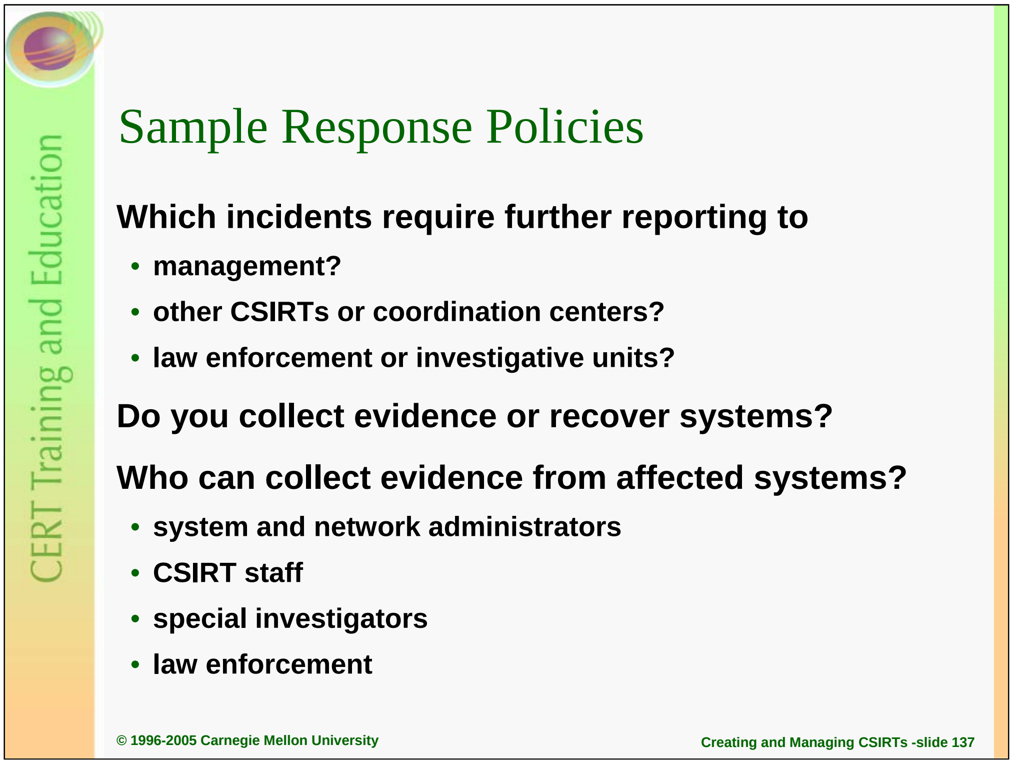
In 2004 and 2005 U. S. Secret Service and CERT/CC published reports on insider threats in the banking and finance sector  and on sabotage by insiders across the critical infrastructure sectors, respectively. These reports draw on case records, investigative reports, and interviews, it analyzes technical 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.
- 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.

Similar information was reported in the second study, *Insider Threat Study: Computer System Sabotage in Critical Infrastructure*. However, this report focused on incidents where the insider purposely attempted to sabotage their company. This report can be found at: http://www.cert.org/archive/pdf/insidercross051105.pdf. Some of the statistics from the report include:

- At the time of the incident 58% of the insiders were former employees or contractors of the affected organizations and 41% were current employees or contractors.
- In 61% of the cases, the insider's actions were limited to relatively unsophisticated methods of attack.
- In 92% of the cases, a specific event or a series of events triggered the insiders' actions (including termination, demotions, transfers, or other disputes)
- In 84% of the cases, the incident was motivated by a desire for revenge.



CERT Training and Education

## Sample Response Policies

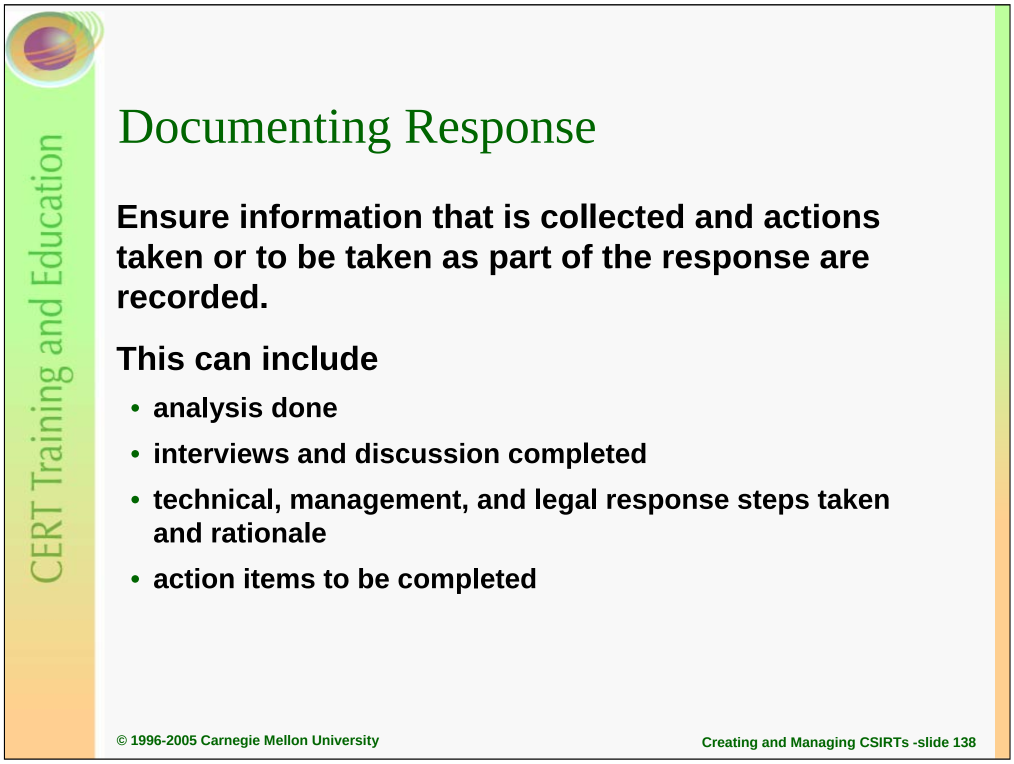
**Which incidents require further reporting to**

- **management?**
- **other CSIRTs or coordination centers?**
- **law enforcement or investigative units?**

**Do you collect evidence or recover systems?**

**Who can collect evidence from affected systems?**

- **system and network administrators**
- **CSIRT staff**
- **special investigators**
- **law enforcement**



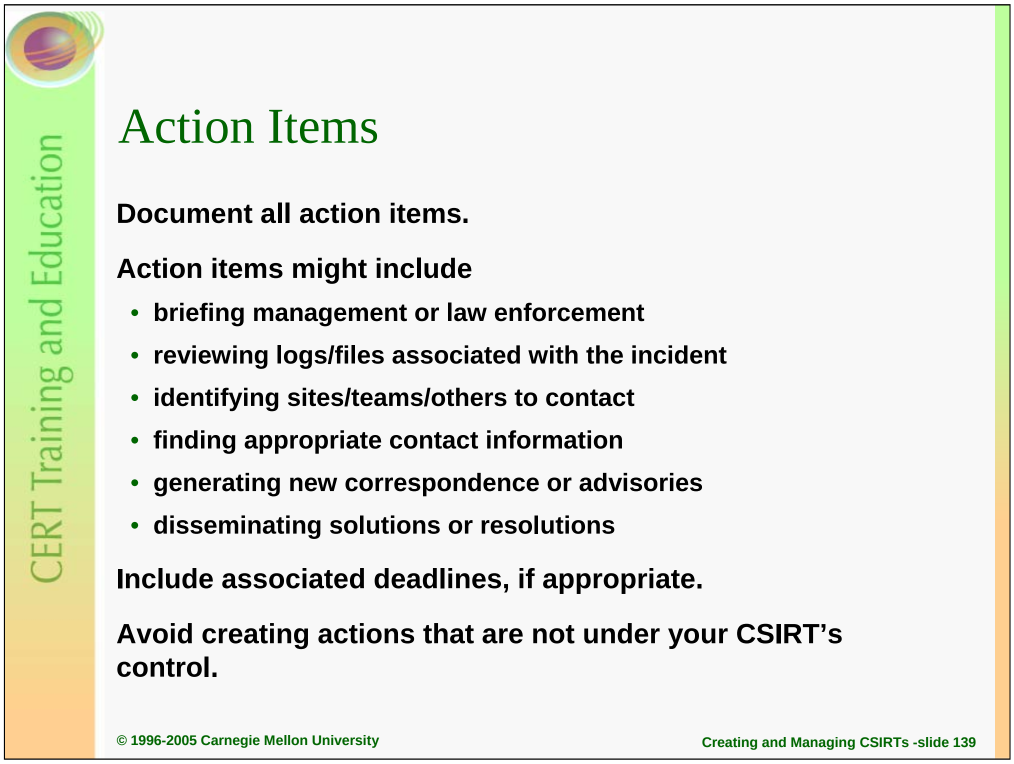
CERT Training and Education

## 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**



CERT Training and Education

# Action Items

**Document all action items.**

**Action items might include**

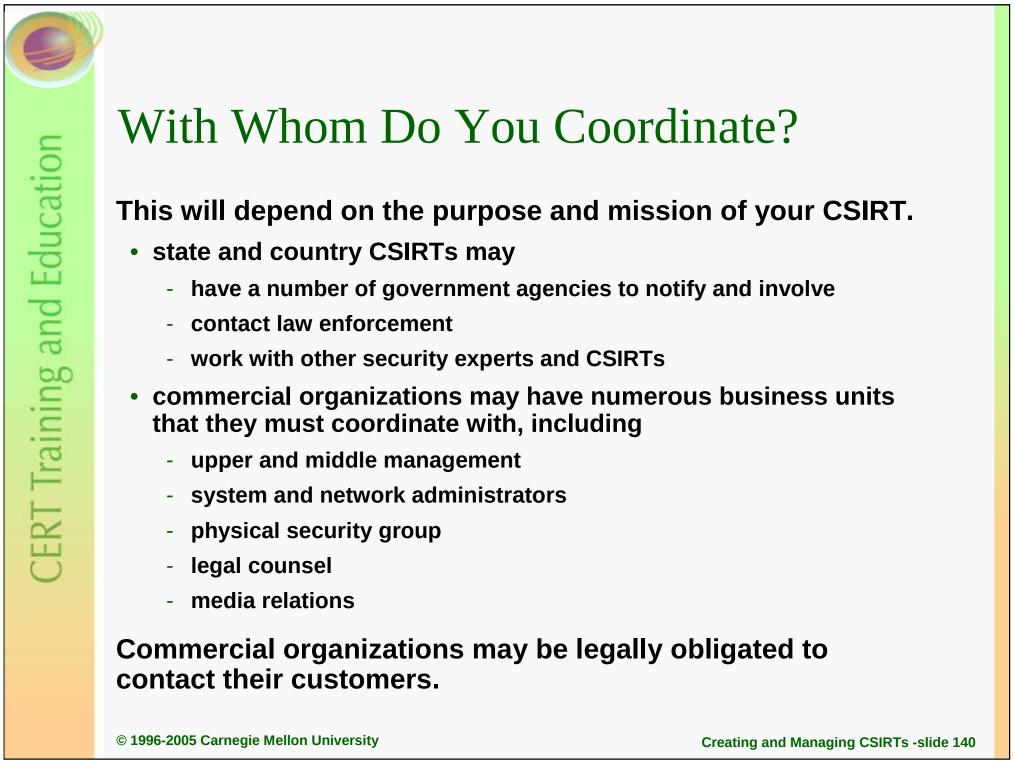
- **briefing management or law enforcement**
- **reviewing logs/files associated with the incident**
- **identifying sites/teams/others to contact**
- **finding appropriate contact information**
- **generating new correspondence or advisories**
- **disseminating solutions or resolutions**

**Include associated deadlines, if appropriate.**

**Avoid creating actions that are not under your CSIRT's control.**

Examples of action items:

- <Moira>: by <Sep 24>, respond to message 1234 from help.site.org. Give pointers to documentation on one-time passwords.
- <Moira>: by <Sep 24>, contact targets of attack (36 sites - only 3 have CSIRTs) in message 1235 using contact info from message 1220 - include sanitized log extracts.
- <Moira>: by <Sep 24>, review 25Mb of intruder logs from help.site.org in email message 1200.


CERT Training and Education

## With Whom Do You Coordinate?

**This will depend on the purpose and mission of your CSIRT.**

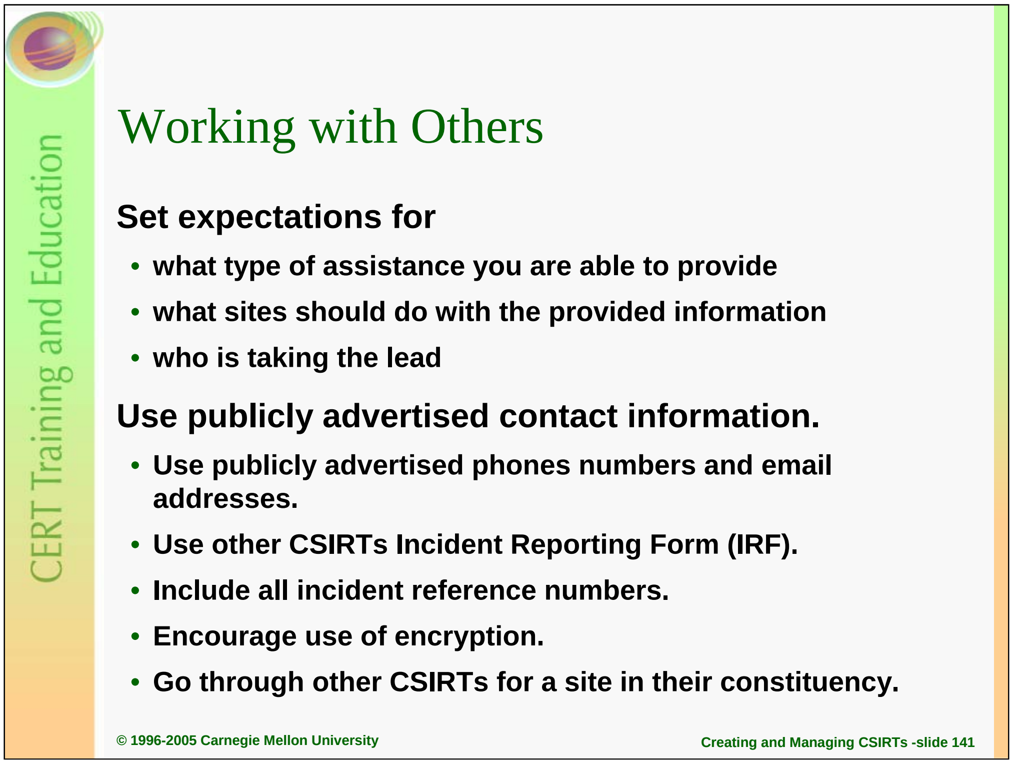
- **state and country CSIRTs may**
  - **have a number of government agencies to notify and involve**
  - **contact law enforcement**
  - **work with other security experts and CSIRTs**
- **commercial organizations may have numerous business units that they must coordinate with, including**
  - **upper and middle management**
  - **system and network administrators**
  - **physical security group**
  - **legal counsel**
  - **media relations**

**Commercial organizations may be legally obligated to contact their customers.**

This will depend on the purpose and mission of your CSIRT.

- state and country CSIRTs may
  - have a number of government agencies to notify and involve
  - contact law enforcement
  - work with other security experts and CSIRTs
- commercial organizations may have numerous business units that they must coordinate with, including
  - upper and middle management
  - system and network administrators
  - physical security group
  - legal counsel
  - media relations

Commercial organizations may be legally obligated to contact their customers.



CERT Training and Education

## Working with Others

**Set expectations for**

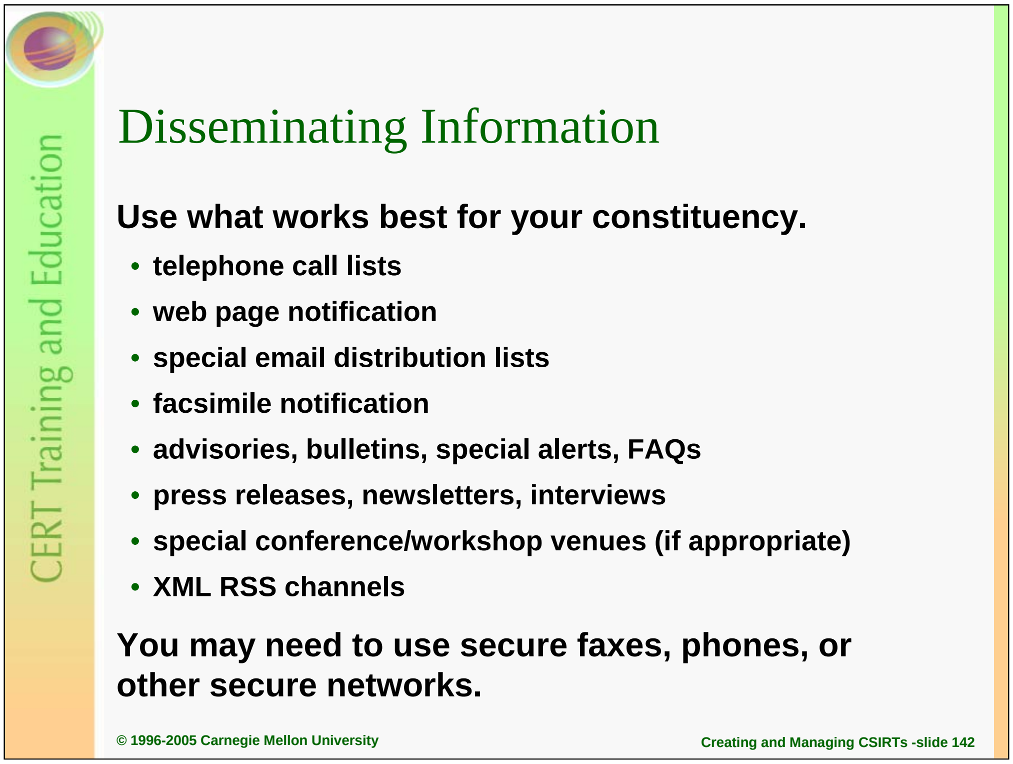
- **what type of assistance you are able to provide**
- **what sites should do with the provided information**
- **who is taking the lead**

**Use publicly advertised contact information.**

- **Use publicly advertised phones numbers and email addresses.**
- **Use other CSIRTs Incident Reporting Form (IRF).**
- **Include all incident reference numbers.**
- **Encourage use of encryption.**
- **Go through other CSIRTs for a site in their constituency.**

Creating and Managing CSIRTs -slide 141

Set expectations for the priorities of your workload, what type of request will get responses, and what type will not.



CERT Training and Education

## Disseminating Information

**Use what works best for your constituency.**

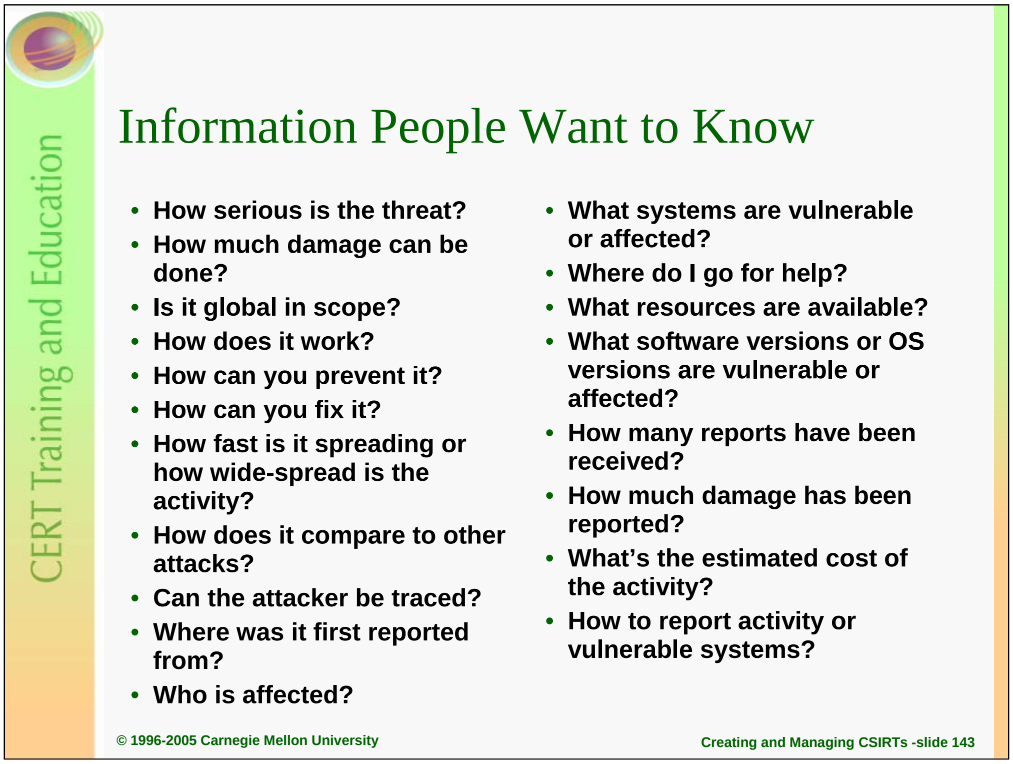
- **telephone call lists**
- **web page notification**
- **special email distribution lists**
- **facsimile notification**
- **advisories, bulletins, special alerts, FAQs**
- **press releases, newsletters, interviews**
- **special conference/workshop venues (if appropriate)**
- **XML RSS channels**

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

Creating and Managing CSIRTs -slide 142

Internally, some CSIRTs have begun using Wiki boards, blogs, and secure chat software to communicate with team members.

JANET has developed a Guidance Note on *Writing Advisories*.
http://www.ja.net/documents/gn_advisories.pdf



CERT Training and Education

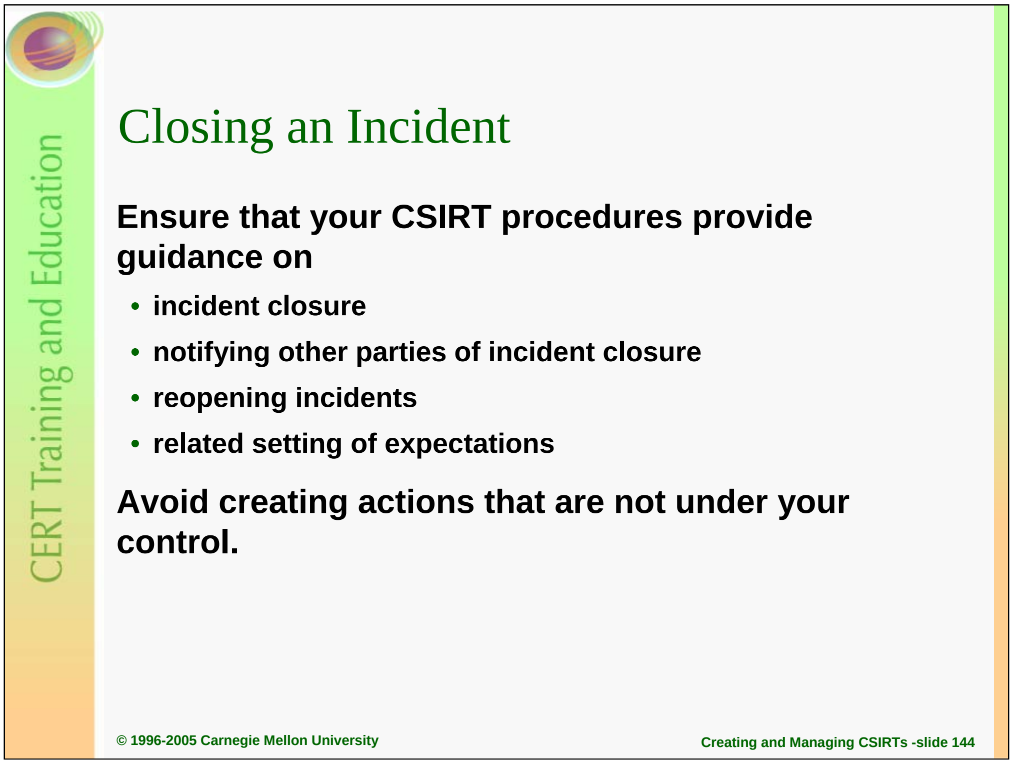
## Information People Want to Know

- 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?

Creating and Managing CSIRTs -slide 143

The above questions can be used to help determine what information you will put in an alert, an advisory, or a post on your web site. These questions can also be used to build an FAQ about any type of incident, vulnerability exploit, or attack.

These are also the types of questions the media will ask.


CERT Training and Education

## Closing an Incident

**Ensure that your CSIRT procedures provide guidance on**

- **incident closure**
- **notifying other parties of incident closure**
- **reopening incidents**
- **related setting of expectations**

**Avoid creating actions that are not under your control.**

Creating and Managing CSIRTs -slide 144

At what point do you determine the closure of an incident? The rationale for closing an incident can differ among other organizations or CSIRTs.

- CERT/CC closes an incident when it is unable to provide any further technical assistance to the sites involved.
- A site may consider an incident open until it recovers and secures its systems or sees no further activity.
- Law enforcement may consider an incident open after a CSIRT and sites consider the incident closed.

Avoid creating actions that are not under your control—for example, an open action that is conditional on a response from someone outside of your CSIRT. The response may never be forthcoming.

How do you inform other involved parties (sites, CSIRTs) that you are closing the incident?

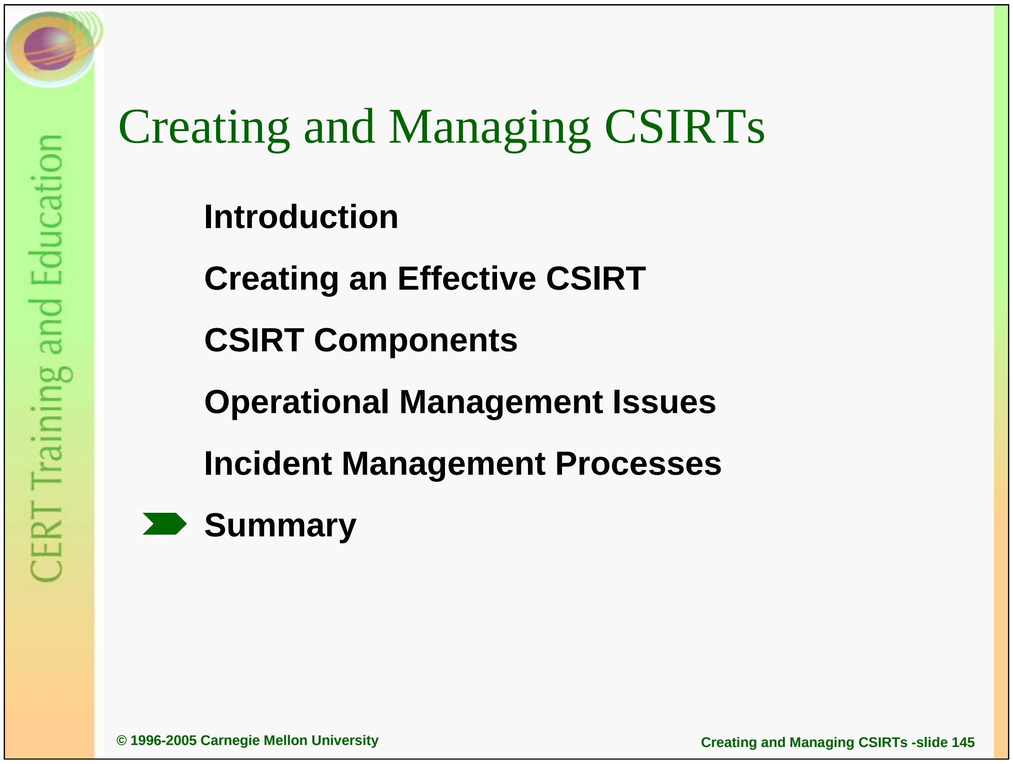
CERT/CC sets expectations via

- a responder message on its cert@cert.org alias
- wording in the CERT/CC Incident Reporting Form
- explicit setting of expectations in direct correspondence with other parties during incident email

The need for reopening closed incidents arises when new information arrives that is clearly related to a closed incident.

CSIRT procedures should cover issues such as

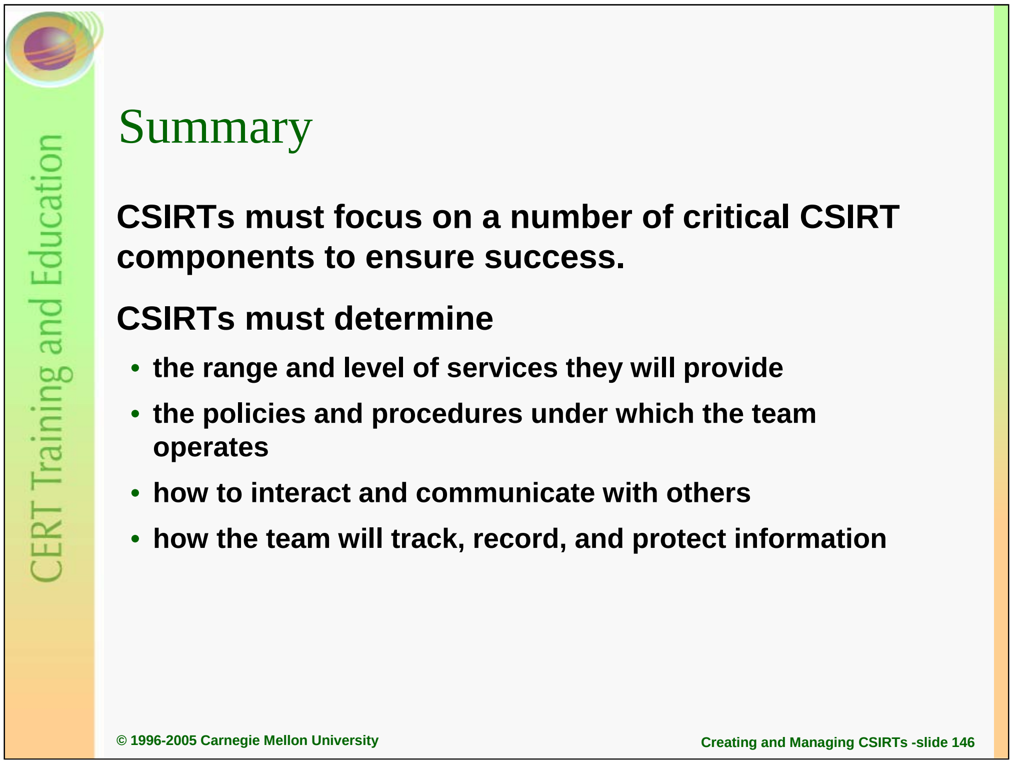
- How will incidents that have been reopened be reviewed or reassigned?
- What reference number will be used for a reopened incident?
- How will a priority be assigned to a reopened incident?



CERT Training and Education

# Creating and Managing CSIRTs

- Introduction
- Creating an Effective CSIRT
- CSIRT Components
- Operational Management Issues
- Incident Management Processes
- ➤ Summary

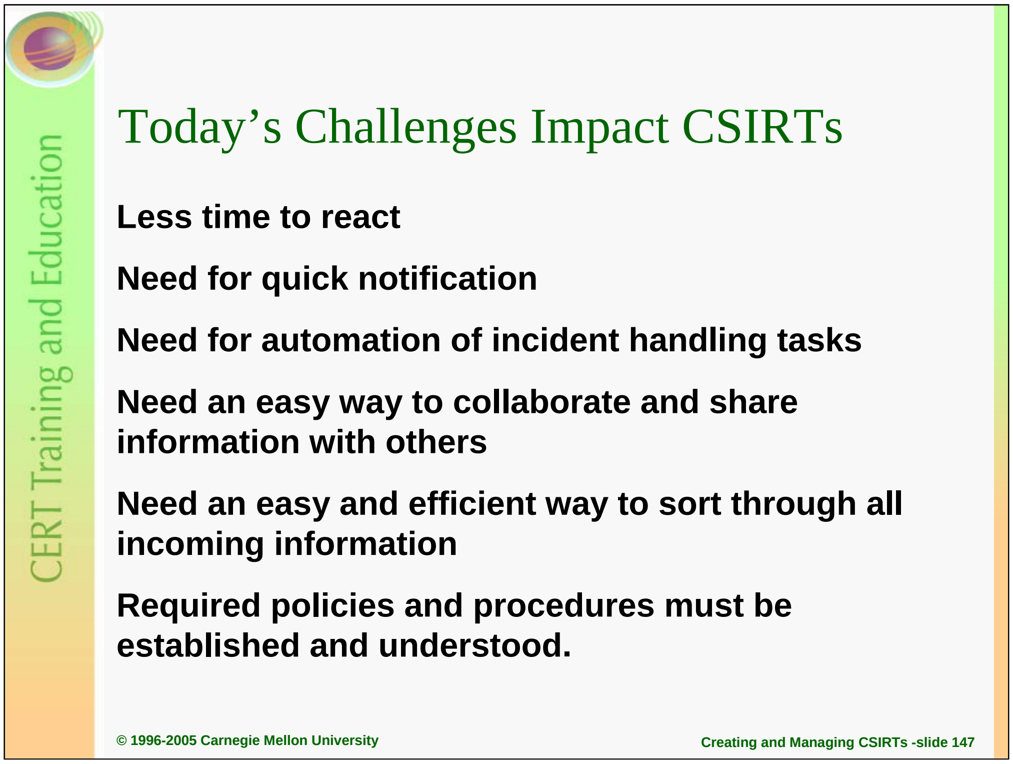

CERT Training and Education

# Summary

**CSIRTs must focus on a number of critical CSIRT components to ensure success.**

**CSIRTs must determine**

- **the range and level of services they will provide**
- **the policies and procedures under which the team operates**
- **how to interact and communicate with others**
- **how the team will track, record, and protect information**

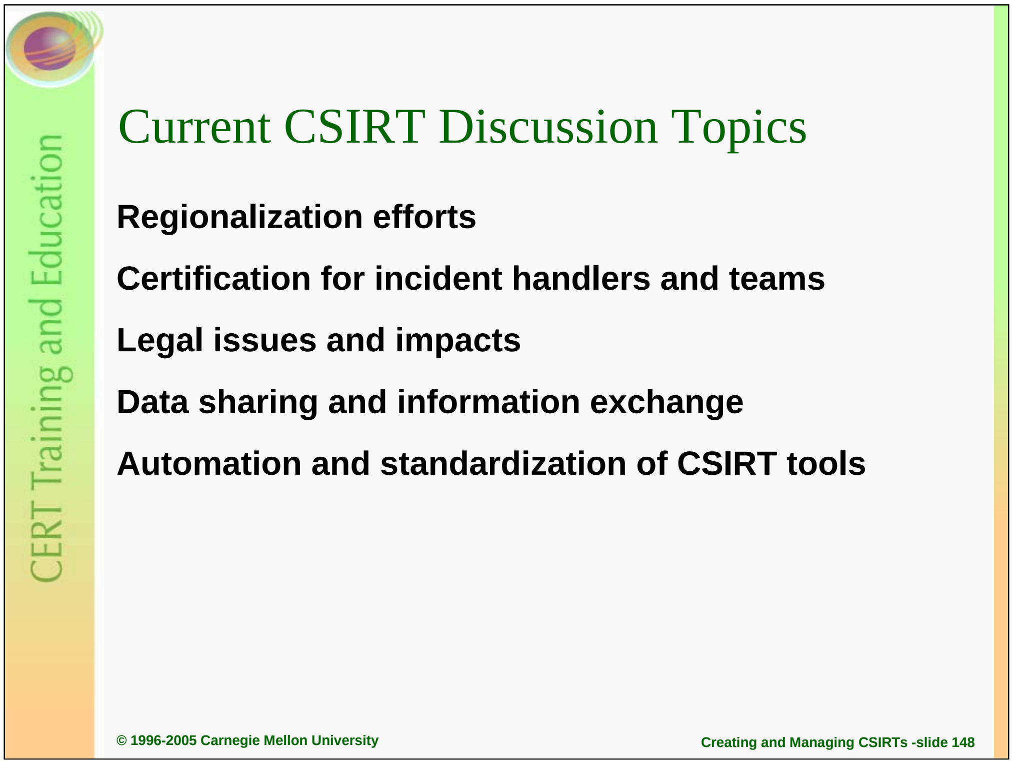


CERT Training and Education

## Today’s Challenges Impact CSIRTs

- Less time to react
- Need for quick notification
- Need for automation of incident handling tasks
- Need an easy way to collaborate and share information with others
- Need an easy and efficient way to sort through all incoming information
- Required policies and procedures must be established and understood.

Creating and Managing CSIRTs -slide 147


CERT Training and Education

## Current CSIRT Discussion Topics

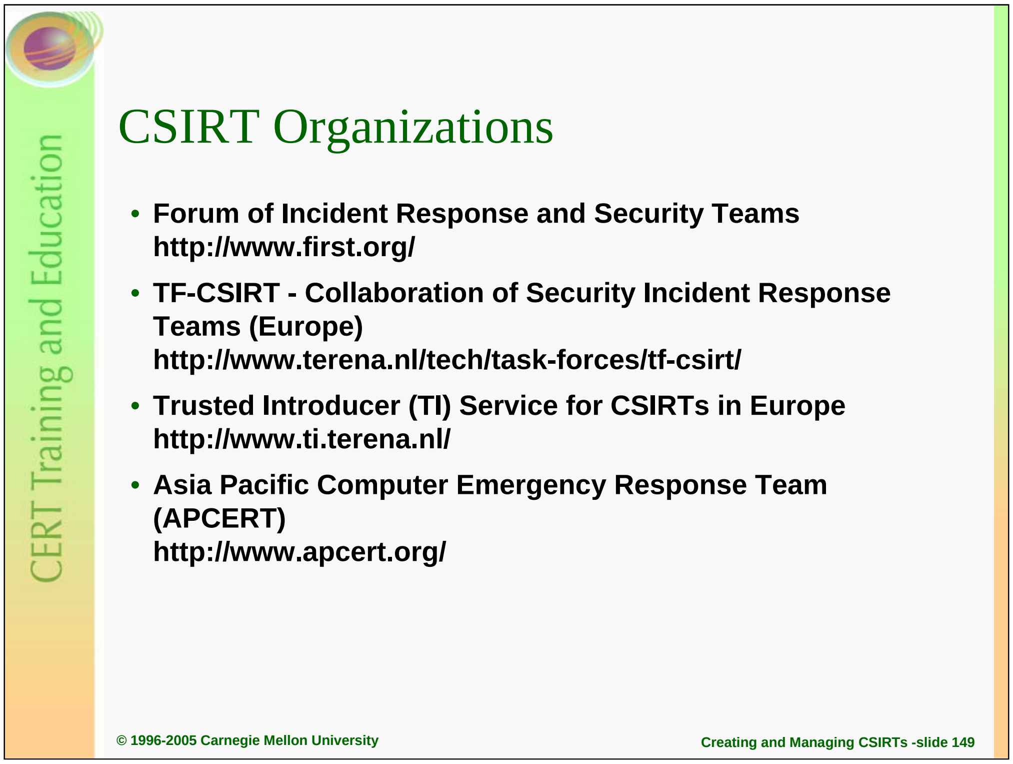
**Regionalization efforts**

**Certification for incident handlers and teams**

**Legal issues and impacts**

**Data sharing and information exchange**

**Automation and standardization of CSIRT tools**



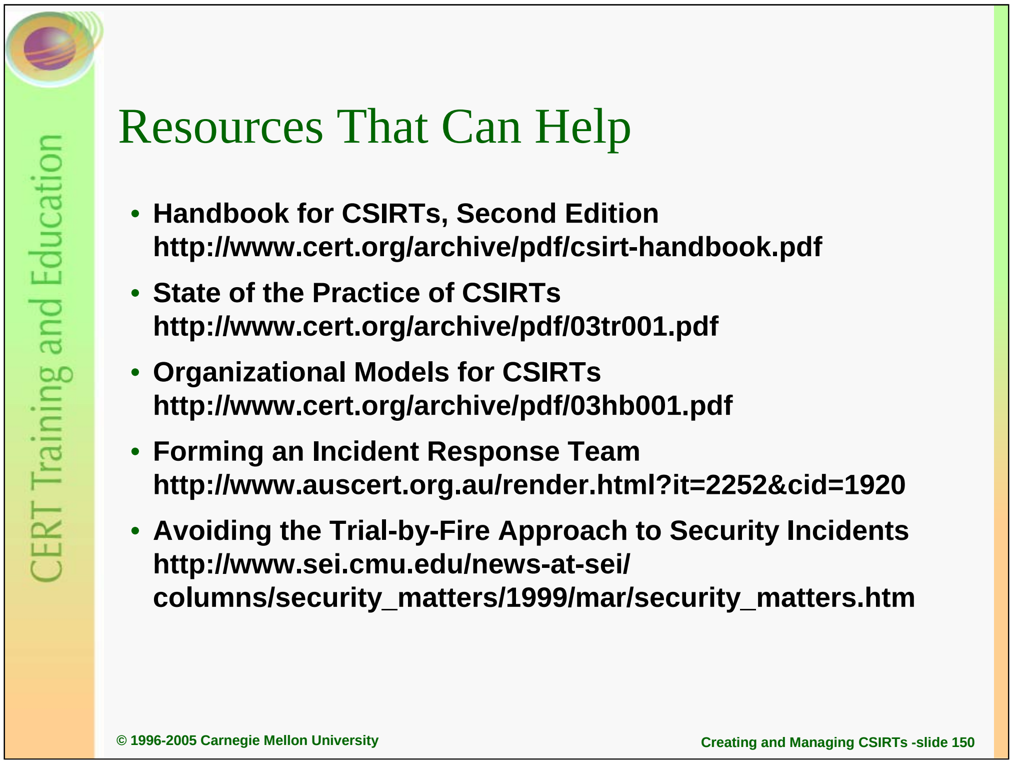
CERT Training and Education

## CSIRT Organizations

- **Forum of Incident Response and Security Teams**
  **http://www.first.org/**
- **TF-CSIRT - Collaboration of Security Incident Response Teams (Europe)**
  **http://www.terena.nl/tech/task-forces/tf-csirt/**
- **Trusted Introducer (TI) Service for CSIRTs in Europe**
  **http://www.ti.terena.nl/**
- **Asia Pacific Computer Emergency Response Team (APCERT)**
  **http://www.apcert.org/**

Creating and Managing CSIRTs -slide 149

- FIRST member teams
  http://www.first.org/team-info/
- TI directory of European CSIRTs
  http://www.ti.terena.nl/teams/
- APCERT members
  http://www.apcert.org/member.html


CERT Training and Education

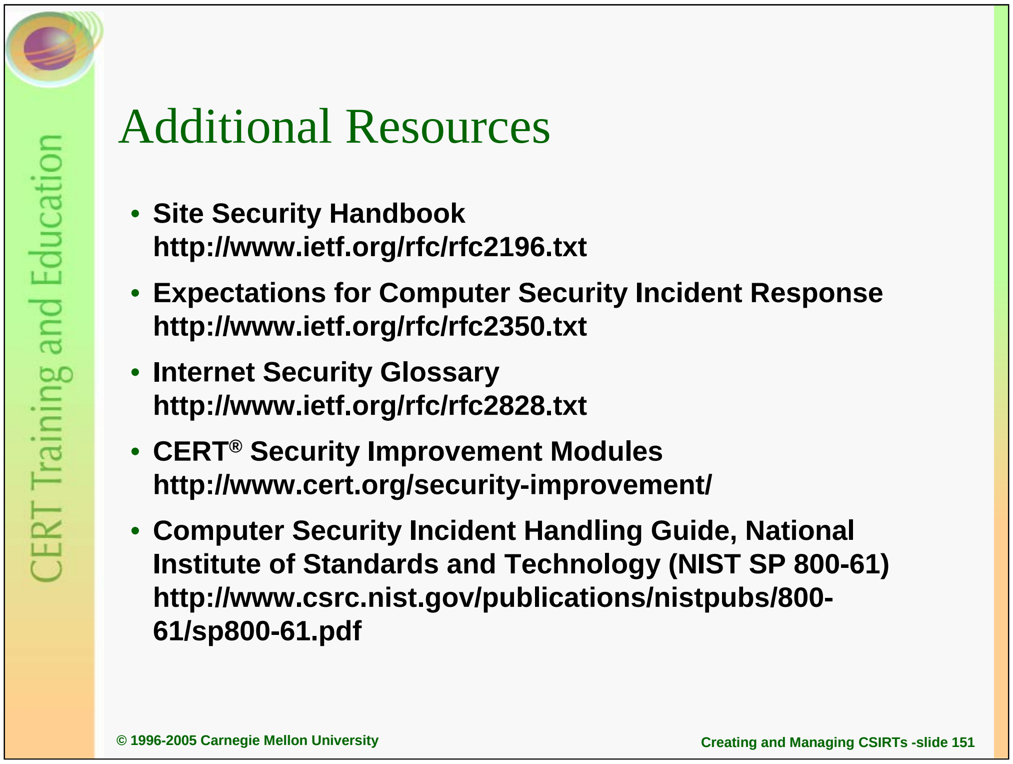
## Resources That Can Help

- **Handbook for CSIRTs, Second Edition**
  **http://www.cert.org/archive/pdf/csirt-handbook.pdf**
- **State of the Practice of CSIRTs**
  **http://www.cert.org/archive/pdf/03tr001.pdf**
- **Organizational Models for CSIRTs**
  **http://www.cert.org/archive/pdf/03hb001.pdf**
- **Forming an Incident Response Team**
  **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**

Creating and Managing CSIRTs -slide 150

Other resources

- CERT® Coordination Center
  http://www.cert.org/
- The SANS (SysAdmin, Audit, Network, Security) Institute
  http://www.sans.org/
- SecurityFocus
  http://www.securityfocus.com/
  http://www.securityfocus.com/incidents
  The SecurityFocus Library archive contains links to many documents, including many in the Incident Handling category http://www.securityfocus.com/library/category/222
- The Center for Education and Research in Information Assurance and Security (CERIAS)
  http://www.cerias.purdue.edu/
- IETF Incident Handling Working Group (INCH WG)
  http://www.ietf.org/html.charters/inch-charter.html



CERT Training and Education

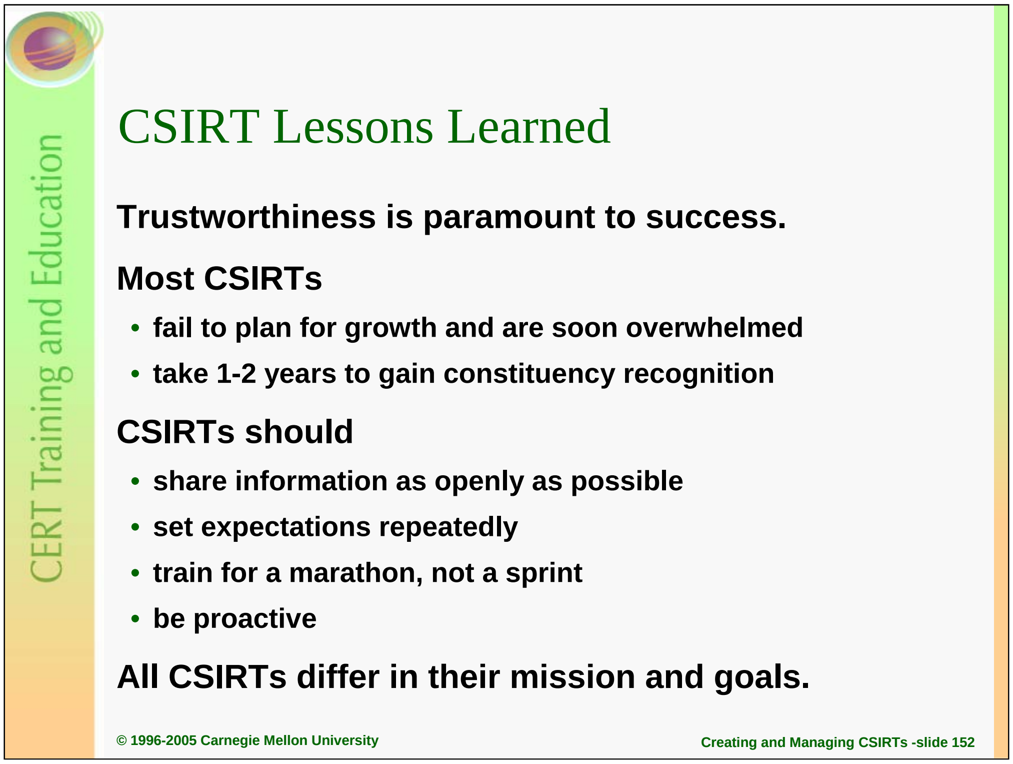
## Additional Resources

- **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**
- **CERT® Security Improvement Modules**
  **http://www.cert.org/security-improvement/**
- **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**

Creating and Managing CSIRTs -slide 151

More resources

- U.S. Computer Emergency Readiness Team (US-CERT)
  http://www.us-cert.gov/
- U.S. Department of Justice Computer Crime and Intellectual Property Section (CCIPS)
  http://www.cybercrime.gov/
- U.S. Federal Bureau of Investigation (FBI) – Field Offices
  http://www.fbi.gov/contact/fo/fo.htm
- JANET Publications
  http://www.ja.net/documents/publication-list-current.pdf



CERT Training and Education

# CSIRT Lessons Learned

**Trustworthiness is paramount to success.**

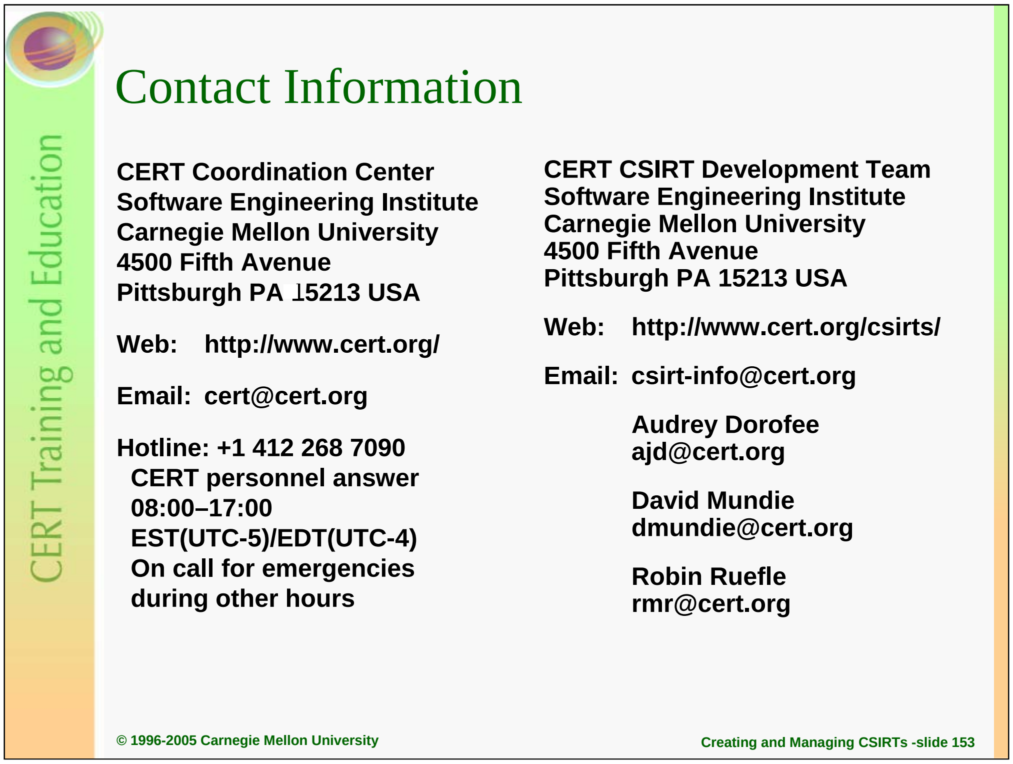
**Most CSIRTs**

- **fail to plan for growth and are soon overwhelmed**
- **take 1-2 years to gain constituency recognition**

**CSIRTs should**

- **share information as openly as possible**
- **set expectations repeatedly**
- **train for a marathon, not a sprint**
- **be proactive**

**All CSIRTs differ in their mission and goals.**


CERT Training and Education

# Contact Information

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

Web: http://www.cert.org/

Email: cert@cert.org

Hotline: +1 412 268 7090
CERT personnel answer
08:00–17:00
EST(UTC-5)/EDT(UTC-4)
On call for emergencies
during other hours

CERT CSIRT Development Team
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

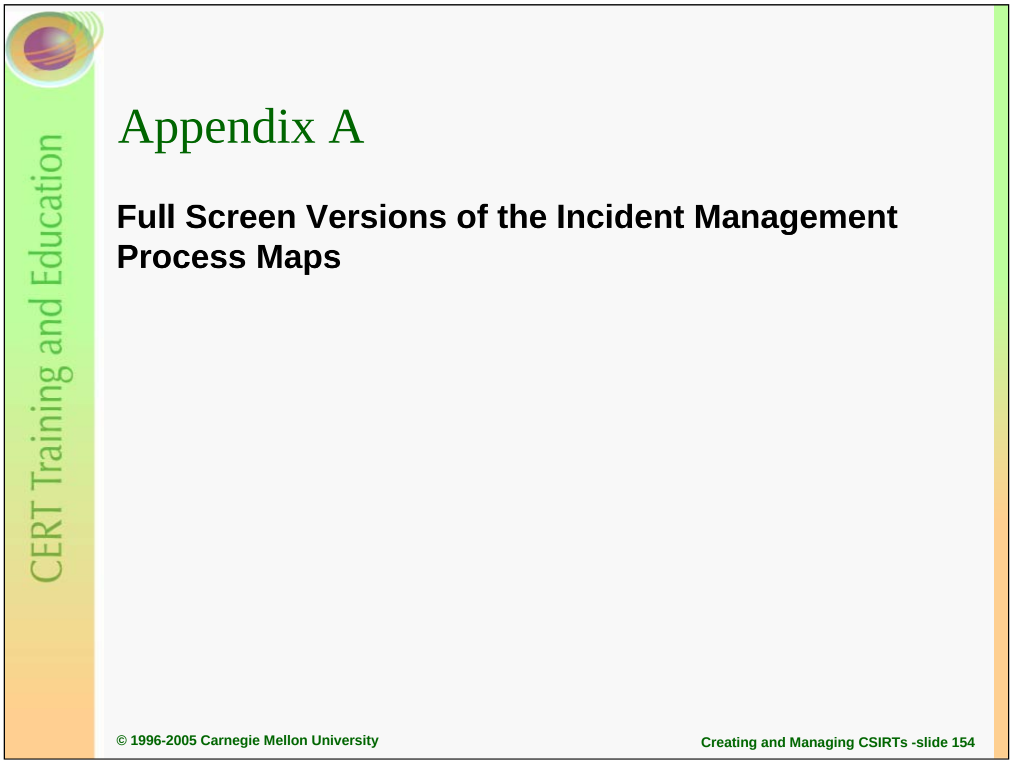
Web: http://www.cert.org/csirts/

Email: csirt-info@cert.org

Audrey Dorofee
ajd@cert.org

David Mundie
dmundie@cert.org

Robin Ruefle
rmr@cert.org

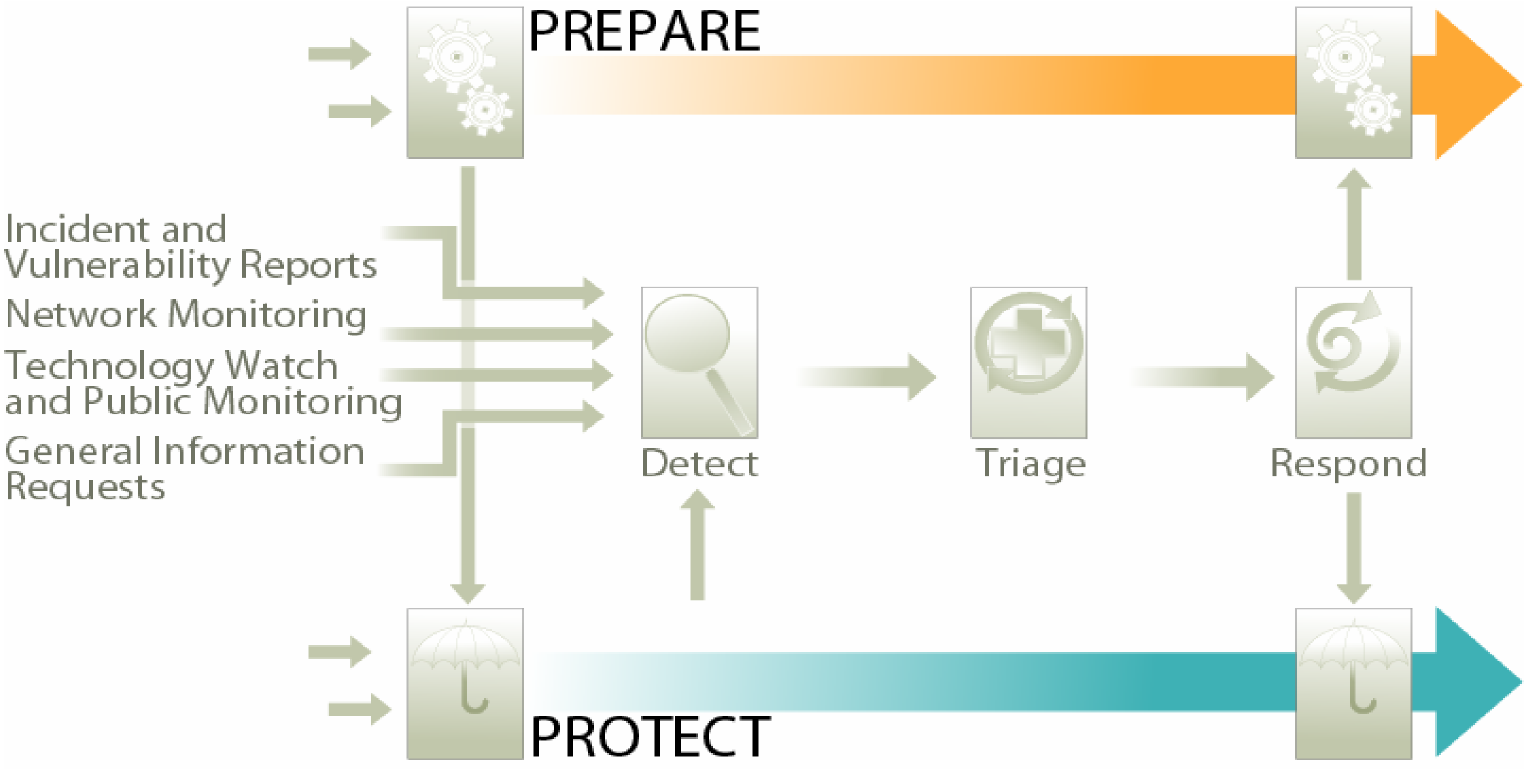


CERT Training and Education

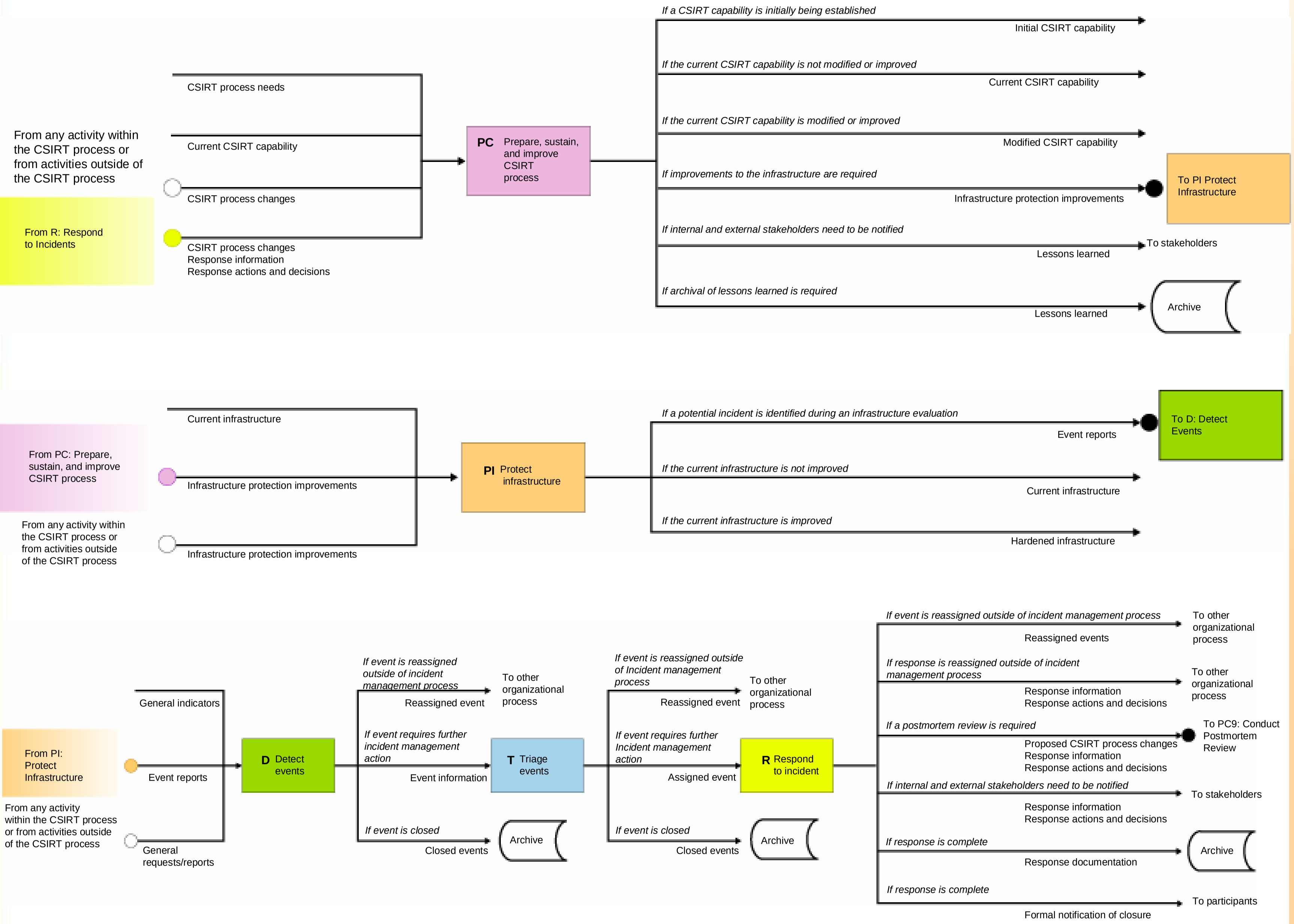
# Appendix A

**Full Screen Versions of the Incident Management Process Maps**

# Incident Management Best Practice Model



# Incident Management



From any activity within the CSIRT process or from activities outside of the CSIRT process

From R: Respond to Incidents

CSIRT process needs

Current CSIRT capability

CSIRT process changes

CSIRT process changes
Response information
Response actions and decisions

PC Prepare, sustain, and improve CSIRT process

If a CSIRT capability is initially being established — Initial CSIRT capability

If the current CSIRT capability is not modified or improved — Current CSIRT capability

If the current CSIRT capability is modified or improved — Modified CSIRT capability

If improvements to the infrastructure are required — Infrastructure protection improvements — To PI Protect Infrastructure

If internal and external stakeholders need to be notified — Lessons learned — To stakeholders

If archival of lessons learned is required — Lessons learned — Archive

From PC: Prepare, sustain, and improve CSIRT process

From any activity within the CSIRT process or from activities outside of the CSIRT process

Current infrastructure

Infrastructure protection improvements

Infrastructure protection improvements

PI Protect infrastructure

If a potential incident is identified during an infrastructure evaluation — Event reports — To D: Detect Events

If the current infrastructure is not improved — Current infrastructure

If the current infrastructure is improved — Hardened infrastructure

From PI: Protect Infrastructure

From any activity within the CSIRT process or from activities outside of the CSIRT process

General indicators

Event reports

General requests/reports

D Detect events

If event is reassigned outside of incident management process — Reassigned event — To other organizational process

If event requires further incident management action — Event information

If event is closed — Closed events — Archive

T Triage events

If event is reassigned outside of Incident management process — Reassigned event — To other organizational process

If event requires further Incident management action — Assigned event

If event is closed — Closed events — Archive

R Respond to incident

If event is reassigned outside of incident management process — Reassigned events — To other organizational process

If response is reassigned outside of incident management process — Response information, Response actions and decisions — To other organizational process

If a postmortem review is required — Proposed CSIRT process changes, Response information, Response actions and decisions — To PC9: Conduct Postmortem Review

If internal and external stakeholders need to be notified — Response information, Response actions and decisions — To stakeholders

If response is complete — Response documentation — Archive

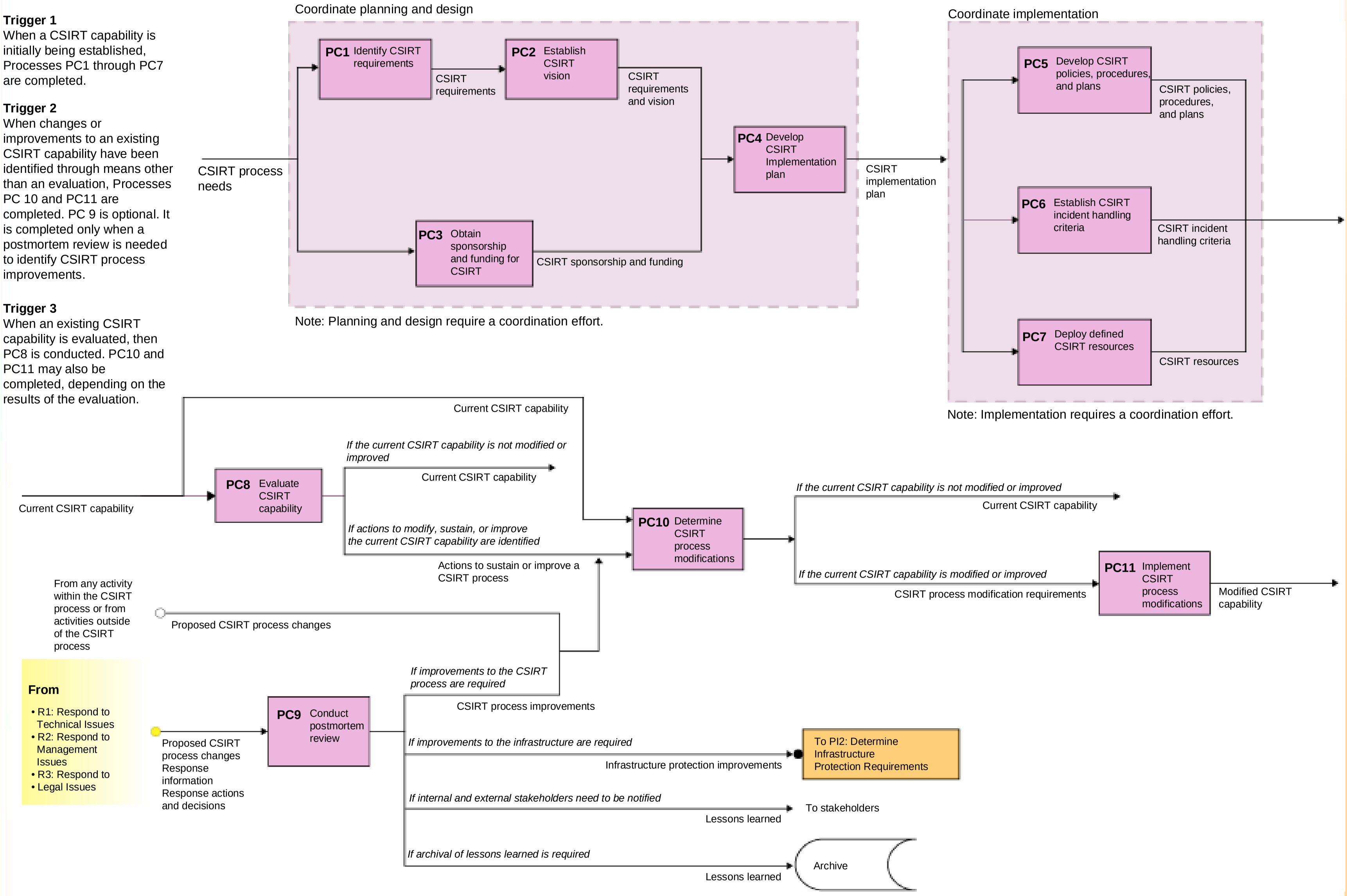
If response is complete — Formal notification of closure — To participants

# 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.

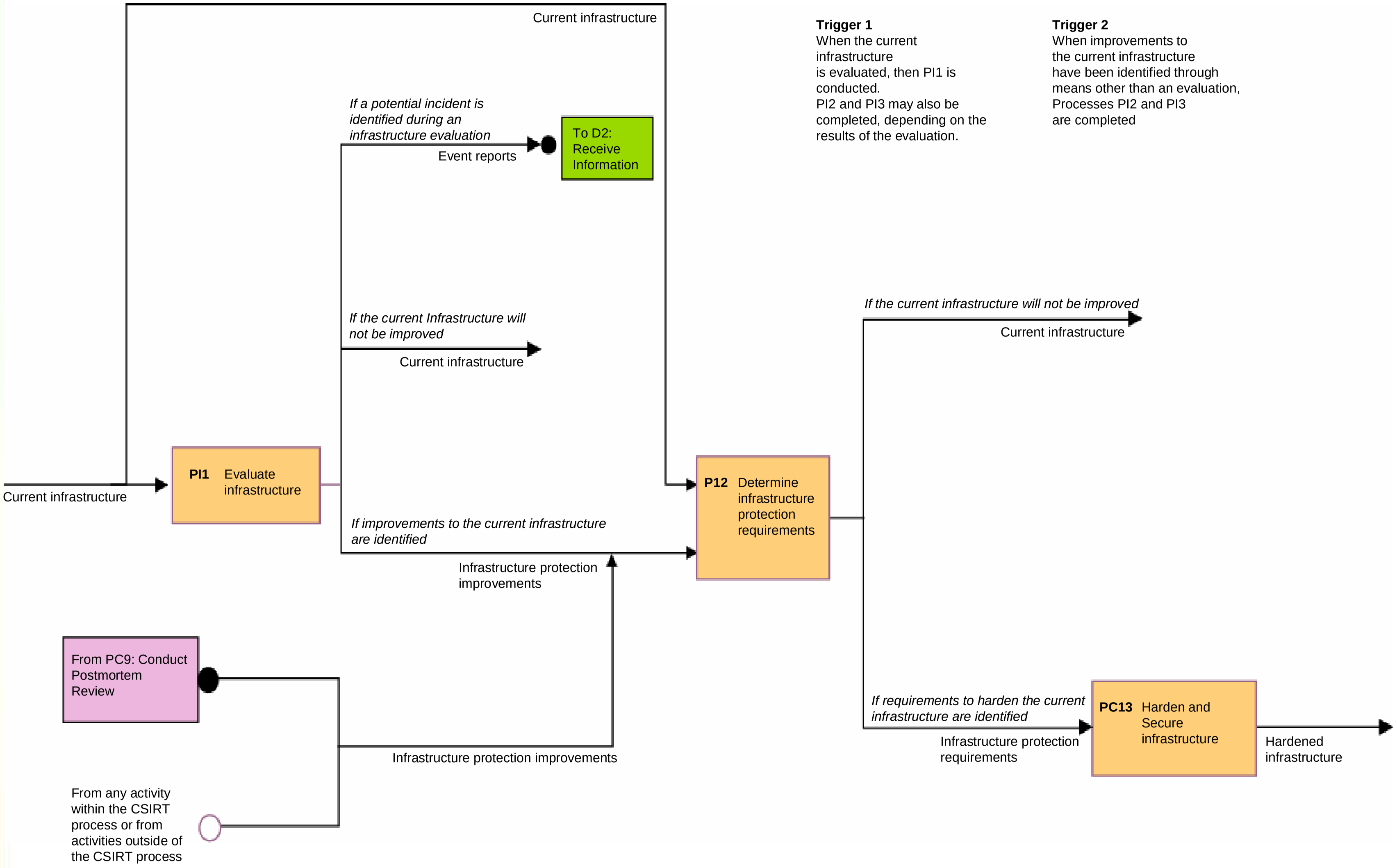
**Trigger 3**
When an existing CSIRT capability is evaluated, then PC8 is conducted. PC10 and PC11 may also be completed, depending on the results of the evaluation.



Coordinate planning and design
CSIRT process needs
PC1 Identify CSIRT requirements
CSIRT requirements
PC2 Establish CSIRT vision
CSIRT requirements and vision
PC3 Obtain sponsorship and funding for CSIRT
CSIRT sponsorship and funding
PC4 Develop CSIRT Implementation plan
CSIRT implementation plan
Note: Planning and design require a coordination effort.
Coordinate implementation
PC5 Develop CSIRT policies, procedures, and plans
CSIRT policies, procedures, and plans
PC6 Establish CSIRT incident handling criteria
CSIRT incident handling criteria
PC7 Deploy defined CSIRT resources
CSIRT resources
Note: Implementation requires a coordination effort.
Current CSIRT capability
Current CSIRT capability
PC8 Evaluate CSIRT capability
If the current CSIRT capability is not modified or improved
Current CSIRT capability
If actions to modify, sustain, or improve the current CSIRT capability are identified
Actions to sustain or improve a CSIRT process
PC10 Determine CSIRT process modifications
If the current CSIRT capability is not modified or improved
Current CSIRT capability
If the current CSIRT capability is modified or improved
CSIRT process modification requirements
PC11 Implement CSIRT process modifications
Modified CSIRT capability
From any activity within the CSIRT process or from activities outside of the CSIRT process
Proposed CSIRT process changes
From
• R1: Respond to Technical Issues
• R2: Respond to Management Issues
• R3: Respond to
• Legal Issues
Proposed CSIRT process changes
Response information
Response actions and decisions
PC9 Conduct postmortem review
If improvements to the CSIRT process are required
CSIRT process improvements
If improvements to the infrastructure are required
Infrastructure protection improvements
To PI2: Determine Infrastructure Protection Requirements
If internal and external stakeholders need to be notified
Lessons learned
To stakeholders
If archival of lessons learned is required
Lessons learned
Archive

© 2004, 2005 Carnegie Mellon University

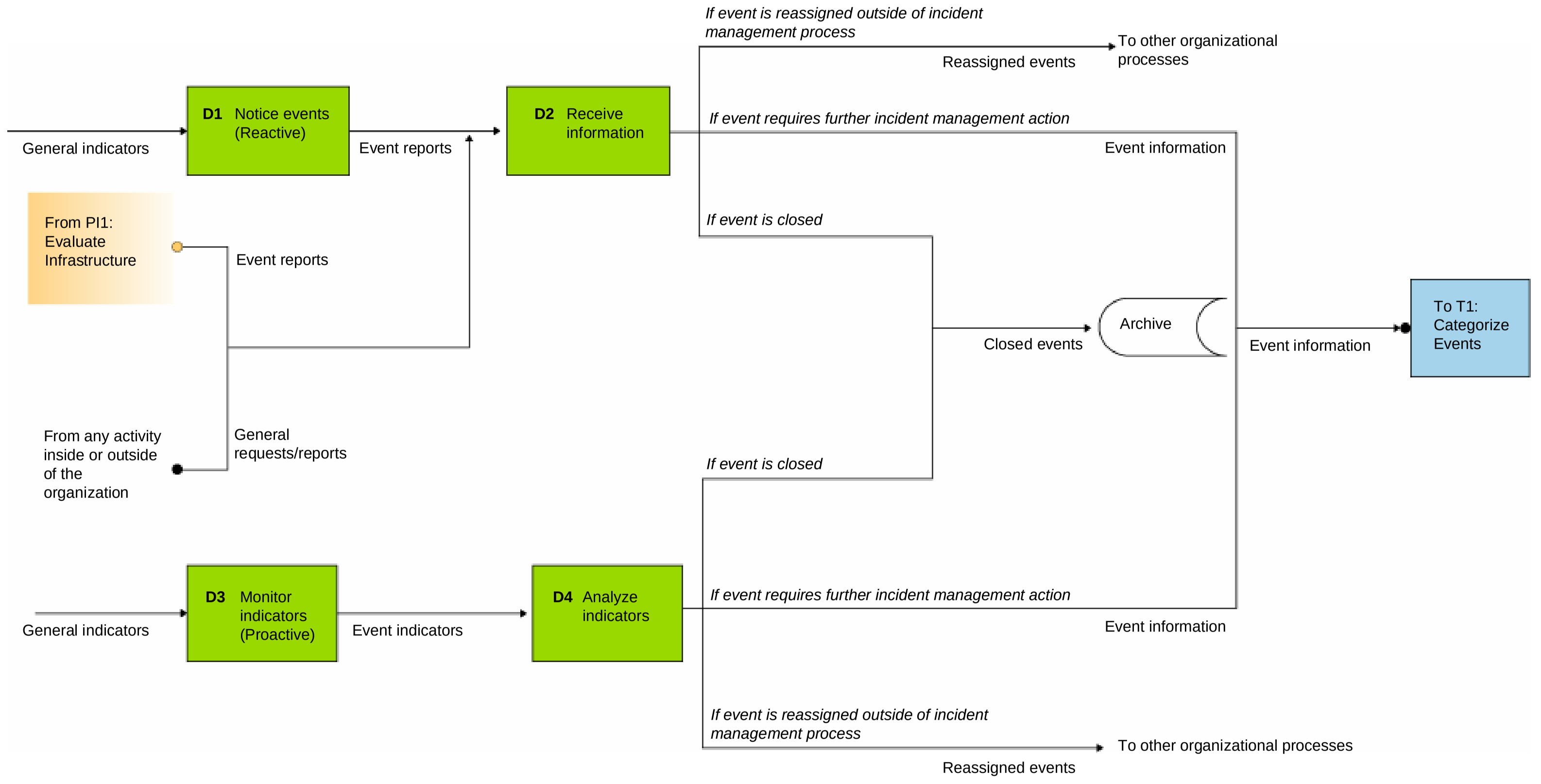
# PI Protect infrastructure


Current infrastructure
Current infrastructure
PI1 Evaluate infrastructure
If a potential incident is identified during an infrastructure evaluation
Event reports
To D2: Receive Information
If the current Infrastructure will not be improved
Current infrastructure
If improvements to the current infrastructure are identified
Infrastructure protection improvements
From PC9: Conduct Postmortem Review
From any activity within the CSIRT process or from activities outside of the CSIRT process
Infrastructure protection improvements
P12 Determine infrastructure protection requirements
If the current infrastructure will not be improved
Current infrastructure
If requirements to harden the current infrastructure are identified
Infrastructure protection requirements
PC13 Harden and Secure infrastructure
Hardened infrastructure

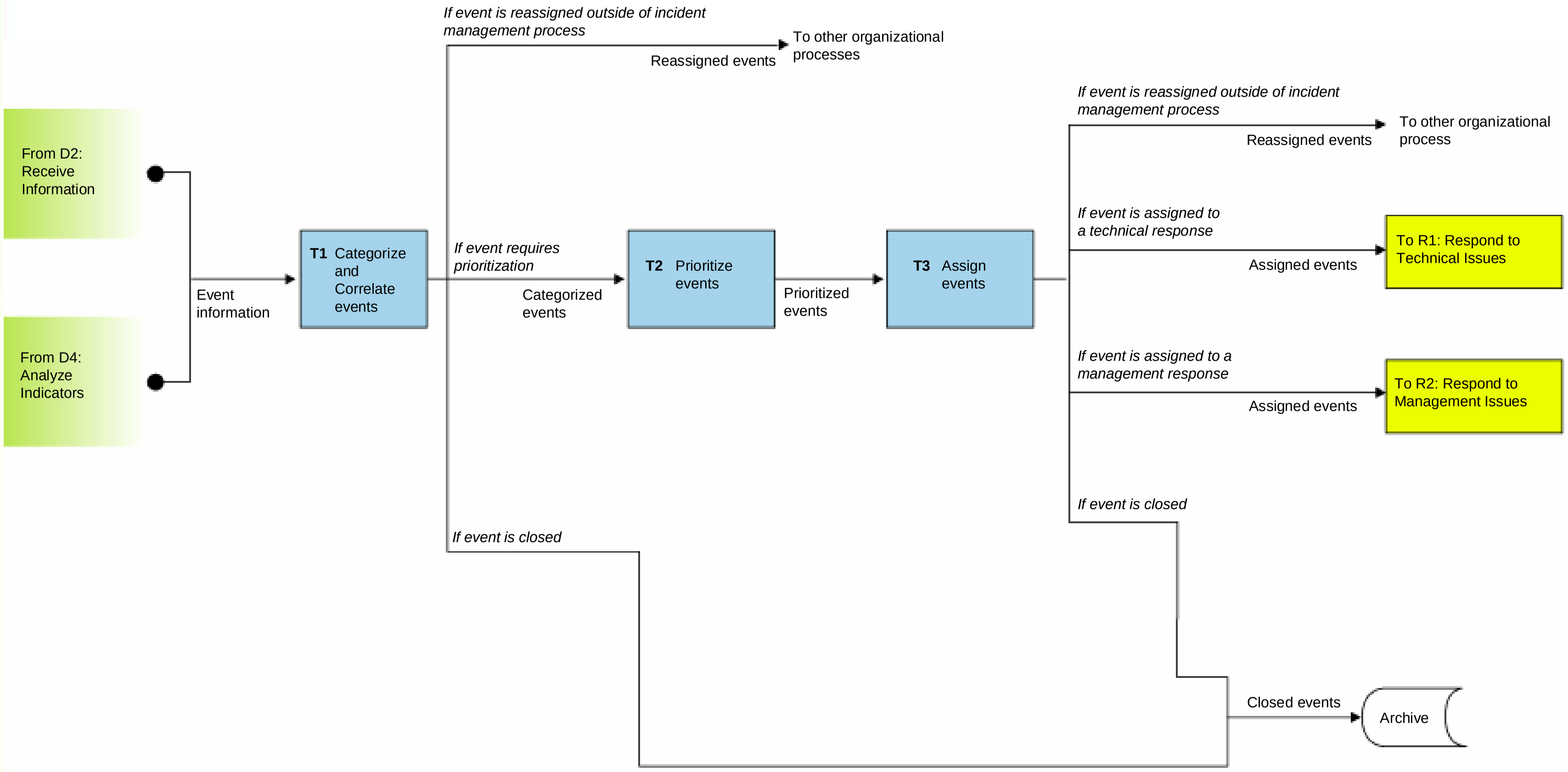
**Trigger 1**
When the current
infrastructure
is evaluated, then PI1 is
conducted.
PI2 and PI3 may also be
completed, depending on the
results of the evaluation.

**Trigger 2**
When improvements to
the current infrastructure
have been identified through
means other than an evaluation,
Processes PI2 and PI3
are completed

# D: Detect Events


General indicators
D1 Notice events (Reactive)
Event reports
D2 Receive information
From PI1: Evaluate Infrastructure
Event reports
From any activity inside or outside of the organization
General requests/reports
General indicators
D3 Monitor indicators (Proactive)
Event indicators
D4 Analyze indicators
If event is reassigned outside of incident management process
Reassigned events
To other organizational processes
If event requires further incident management action
Event information
If event is closed
Closed events
Archive
Event information
To T1: Categorize Events
If event is closed
If event requires further incident management action
Event information
If event is reassigned outside of incident management process
Reassigned events
To other organizational processes

# T: Triage Events



From D2: Receive Information

From D4: Analyze Indicators

Event information

**T1** Categorize and Correlate events

If event is reassigned outside of incident management process

Reassigned events

To other organizational processes

If event requires prioritization

Categorized events

**T2** Prioritize events

Prioritized events

**T3** Assign events

If event is closed

If event is reassigned outside of incident management process

Reassigned events

To other organizational process

If event is assigned to a technical response

Assigned events

To R1: Respond to Technical Issues

If event is assigned to a management response

Assigned events

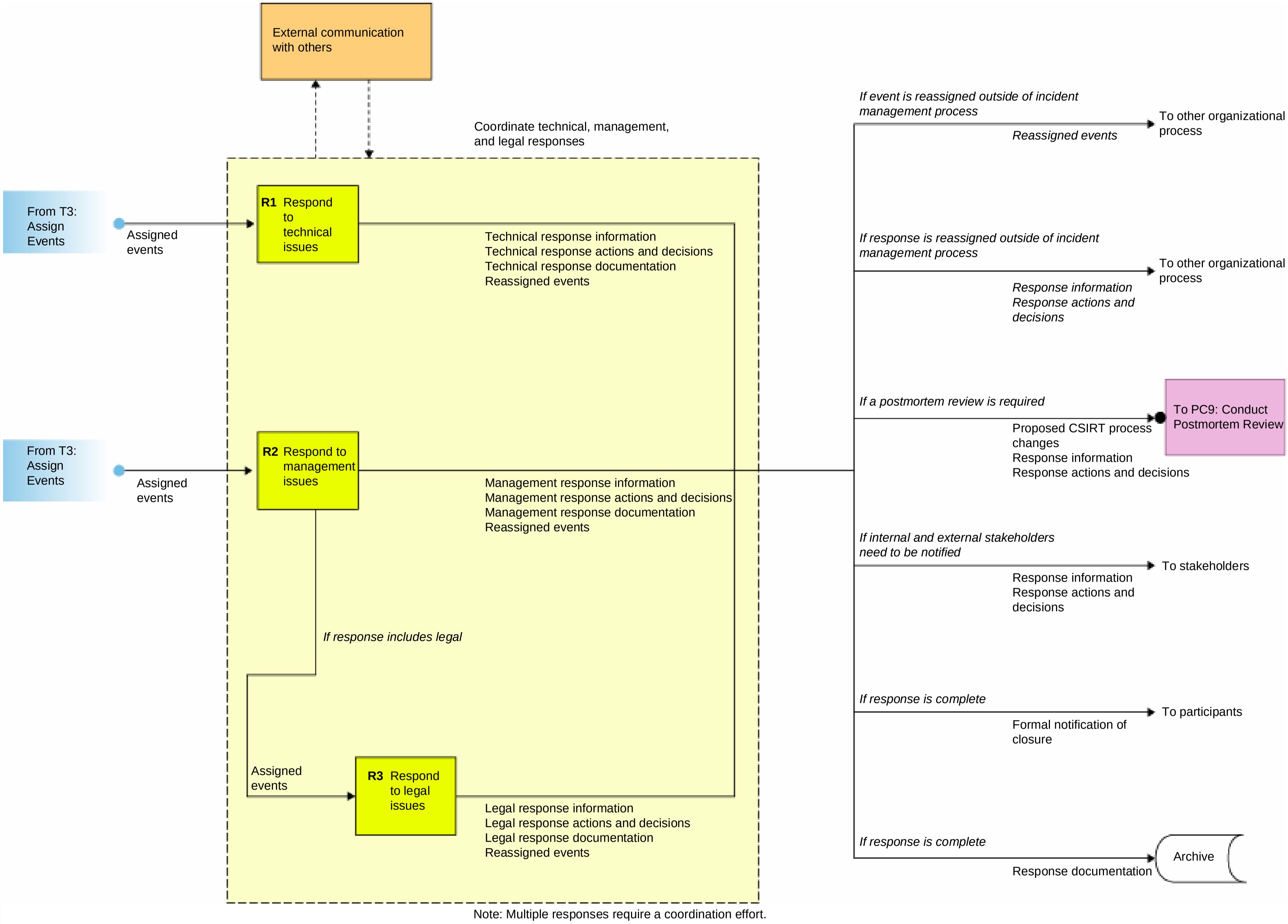
To R2: Respond to Management Issues

If event is closed

Closed events

Archive

# R: Respond



External communication with others

Coordinate technical, management, and legal responses

From T3: Assign Events

Assigned events

**R1** Respond to technical issues

Technical response information
Technical response actions and decisions
Technical response documentation
Reassigned events

From T3: Assign Events

Assigned events

**R2** Respond to management issues

Management response information
Management response actions and decisions
Management response documentation
Reassigned events

*If response includes legal*

Assigned events

**R3** Respond to legal issues

Legal response information
Legal response actions and decisions
Legal response documentation
Reassigned events

*If event is reassigned outside of incident management process*

*Reassigned events*

To other organizational process

*If response is reassigned outside of incident management process*

*Response information*
*Response actions and decisions*

To other organizational process

*If a postmortem review is required*

Proposed CSIRT process changes
Response information
Response actions and decisions

To PC9: Conduct Postmortem Review

*If internal and external stakeholders need to be notified*

Response information
Response actions and decisions

To stakeholders

*If response is complete*

Formal notification of closure

To participants

*If response is complete*

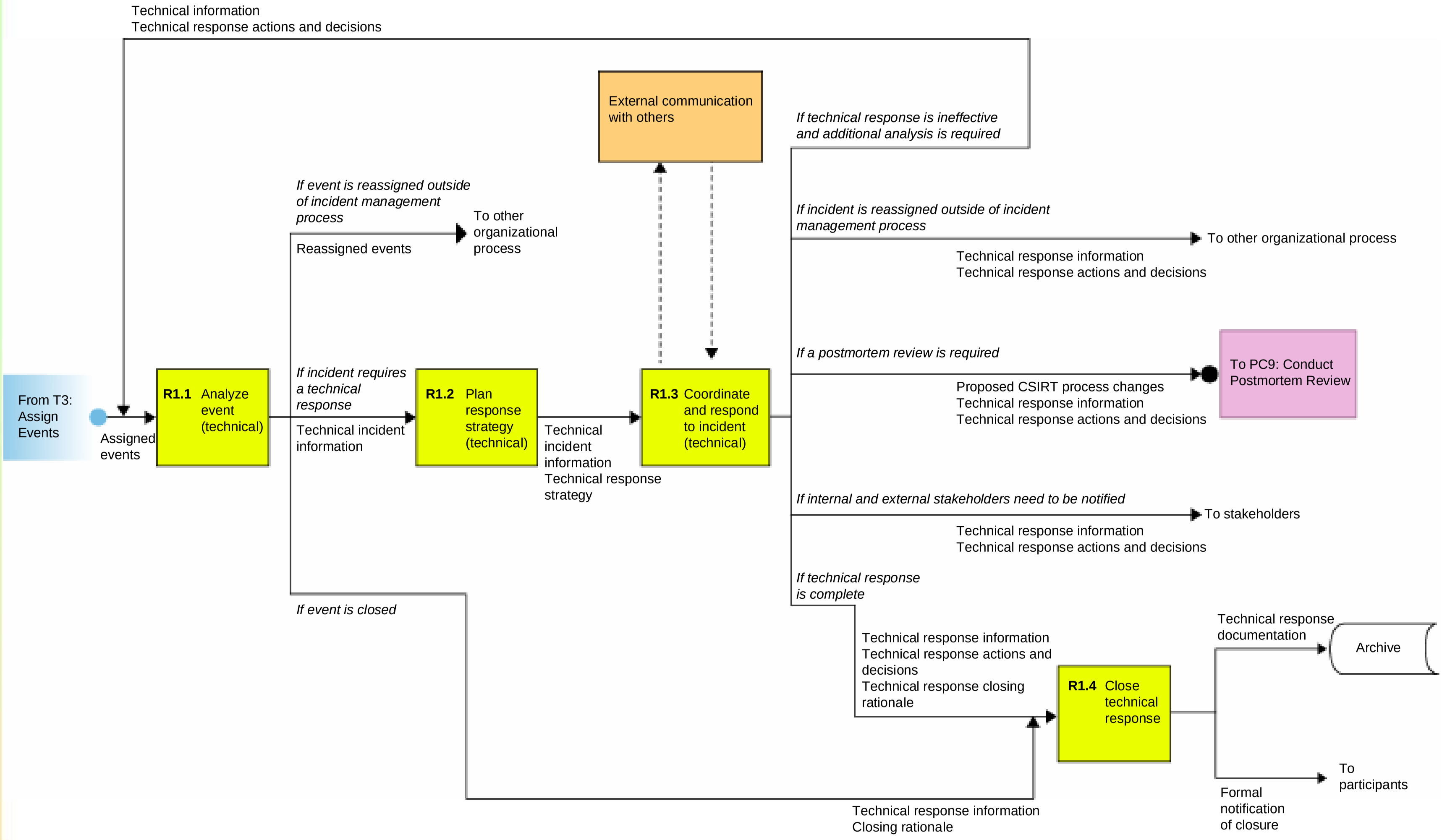
Response documentation

Archive

Note: Multiple responses require a coordination effort.

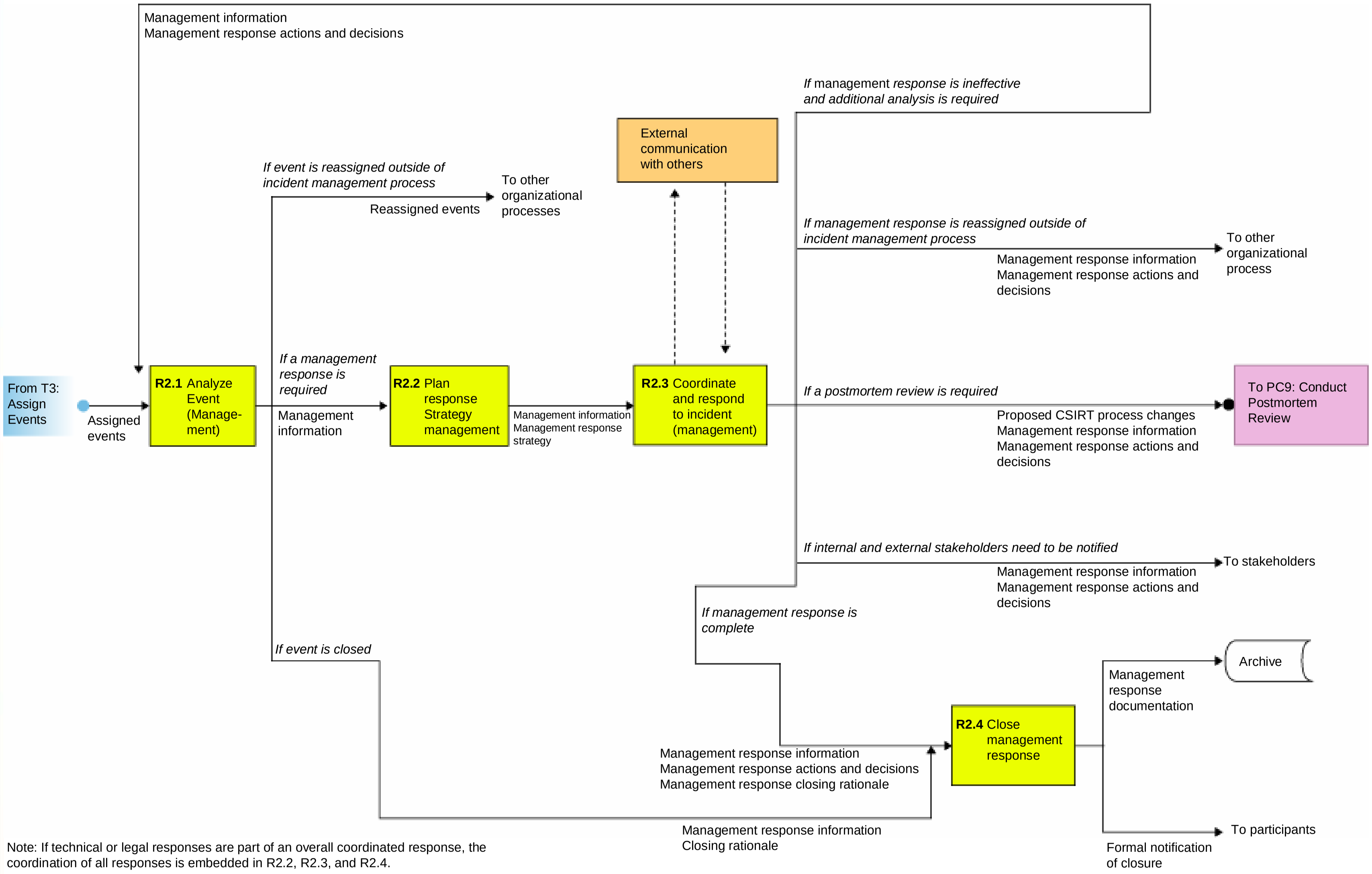
CERT Training and Education

# R1: Respond to Technical Issues


Technical information
Technical response actions and decisions
From T3: Assign Events
Assigned events
R1.1 Analyze event (technical)
If event is reassigned outside of incident management process
Reassigned events
To other organizational process
If incident requires a technical response
Technical incident information
R1.2 Plan response strategy (technical)
Technical incident information
Technical response strategy
External communication with others
R1.3 Coordinate and respond to incident (technical)
If event is closed
If technical response is ineffective and additional analysis is required
If incident is reassigned outside of incident management process
To other organizational process
Technical response information
Technical response actions and decisions
If a postmortem review is required
To PC9: Conduct Postmortem Review
Proposed CSIRT process changes
Technical response information
Technical response actions and decisions
If internal and external stakeholders need to be notified
To stakeholders
Technical response information
Technical response actions and decisions
If technical response is complete
Technical response information
Technical response actions and decisions
Technical response closing rationale
R1.4 Close technical response
Technical response information
Closing rationale
Technical response documentation
Archive
Formal notification of closure
To participants

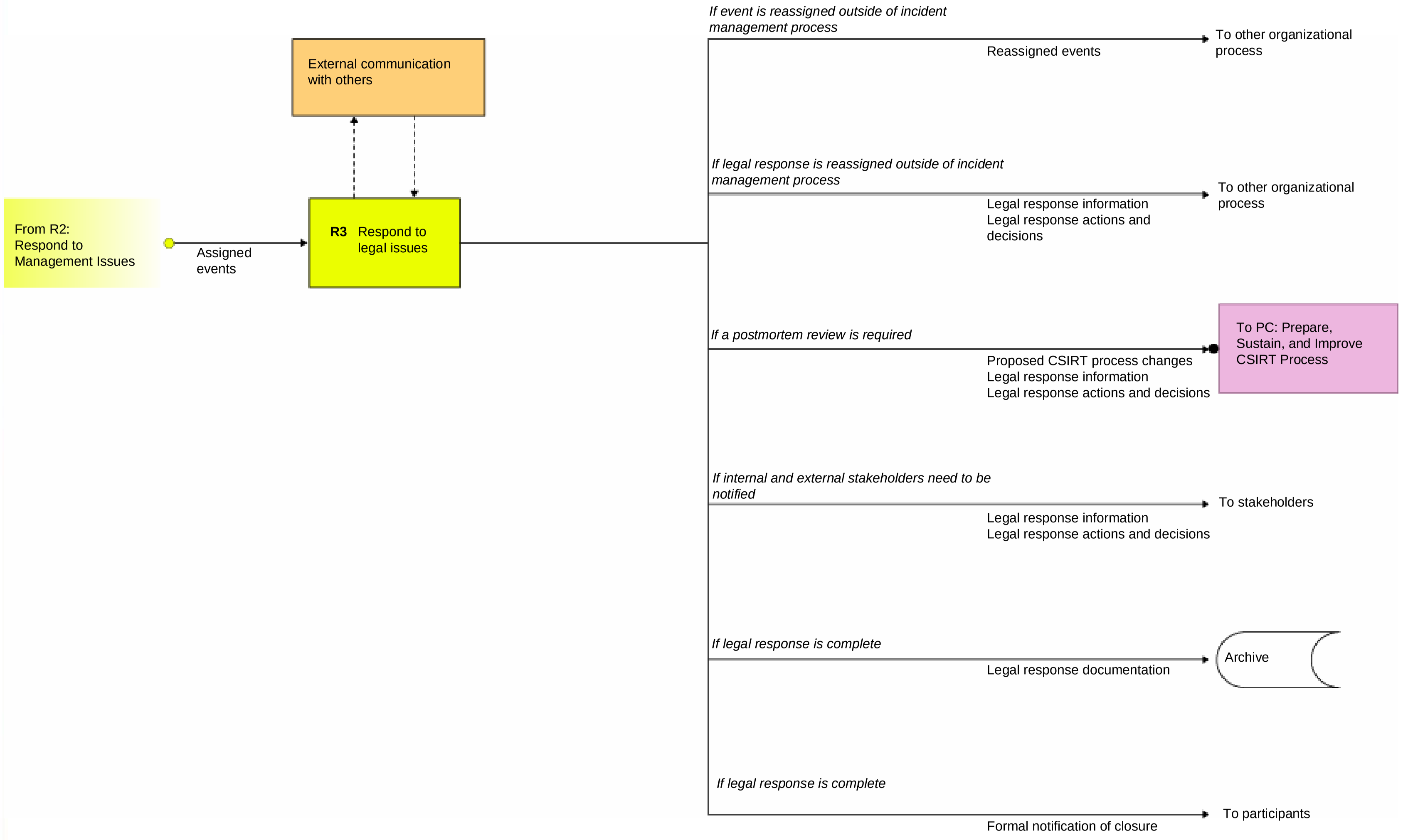
Note: If management or legal responses are part of an overall coordinated response, the coordination of all responses is embedded in R1.2, R1.3, and R1.4.

# R2: Respond to Management Issues


From T3: Assign Events
Assigned events
R2.1 Analyze Event (Manage-ment)
Management information
Management response actions and decisions
If a management response is required
Management information
If event is reassigned outside of incident management process
Reassigned events
To other organizational processes
If event is closed
R2.2 Plan response Strategy management
Management information
Management response strategy
R2.3 Coordinate and respond to incident (management)
External communication with others
If management response is ineffective and additional analysis is required
If management response is reassigned outside of incident management process
Management response information
Management response actions and decisions
To other organizational process
If a postmortem review is required
Proposed CSIRT process changes
Management response information
Management response actions and decisions
To PC9: Conduct Postmortem Review
If internal and external stakeholders need to be notified
Management response information
Management response actions and decisions
To stakeholders
If management response is complete
Management response information
Management response actions and decisions
Management response closing rationale
Management response information
Closing rationale
R2.4 Close management response
Management response documentation
Archive
Formal notification of closure
To participants

Note: If technical or legal responses are part of an overall coordinated response, the coordination of all responses is embedded in R2.2, R2.3, and R2.4.

# R3: Respond to Legal Issues



From R2:
Respond to
Management Issues

Assigned events

External communication with others

**R3** Respond to legal issues

*If event is reassigned outside of incident management process*
Reassigned events
To other organizational process

*If legal response is reassigned outside of incident management process*
Legal response information
Legal response actions and decisions
To other organizational process

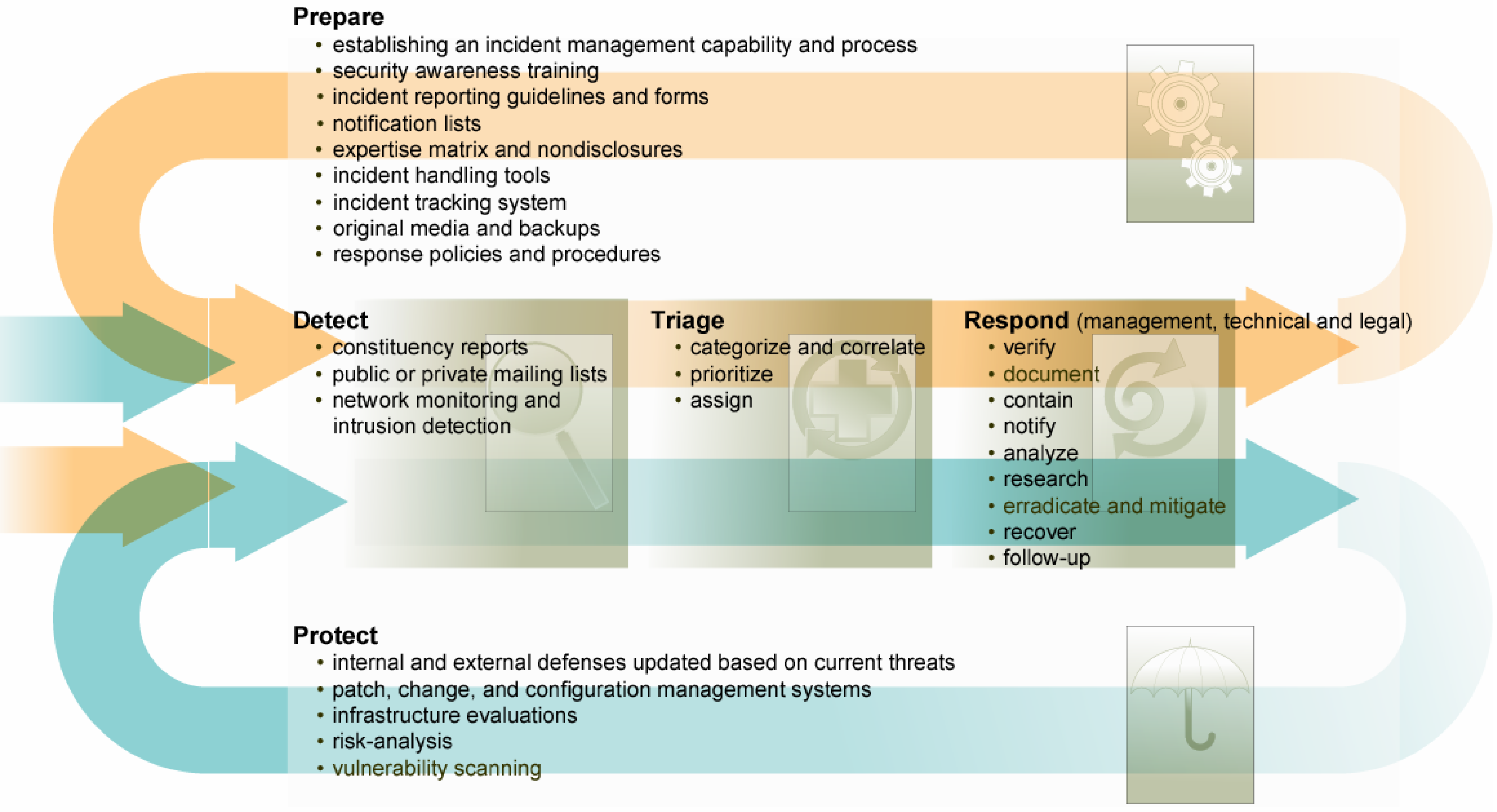
*If a postmortem review is required*
Proposed CSIRT process changes
Legal response information
Legal response actions and decisions
To PC: Prepare, Sustain, and Improve CSIRT Process

*If internal and external stakeholders need to be notified*
Legal response information
Legal response actions and decisions
To stakeholders

*If legal response is complete*
Legal response documentation
Archive

*If legal response is complete*
Formal notification of closure
To participants

# Incident Response Starts Before an Incident Occurs



**Prepare**
- establishing an incident management capability and process
- security awareness training
- incident reporting guidelines and forms
- notification lists
- expertise matrix and nondisclosures
- incident handling tools
- incident tracking system
- original media and backups
- response policies and procedures

**Detect**
- constituency reports
- public or private mailing lists
- network monitoring and intrusion detection

**Triage**
- categorize and correlate
- prioritize
- assign

**Respond** (management, technical and legal)
- verify
- document
- contain
- notify
- analyze
- research
- erradicate and mitigate
- recover
- follow-up

**Protect**
- internal and external defenses updated based on current threats
- patch, change, and configuration management systems
- infrastructure evaluations
- risk-analysis
- vulnerability scanning