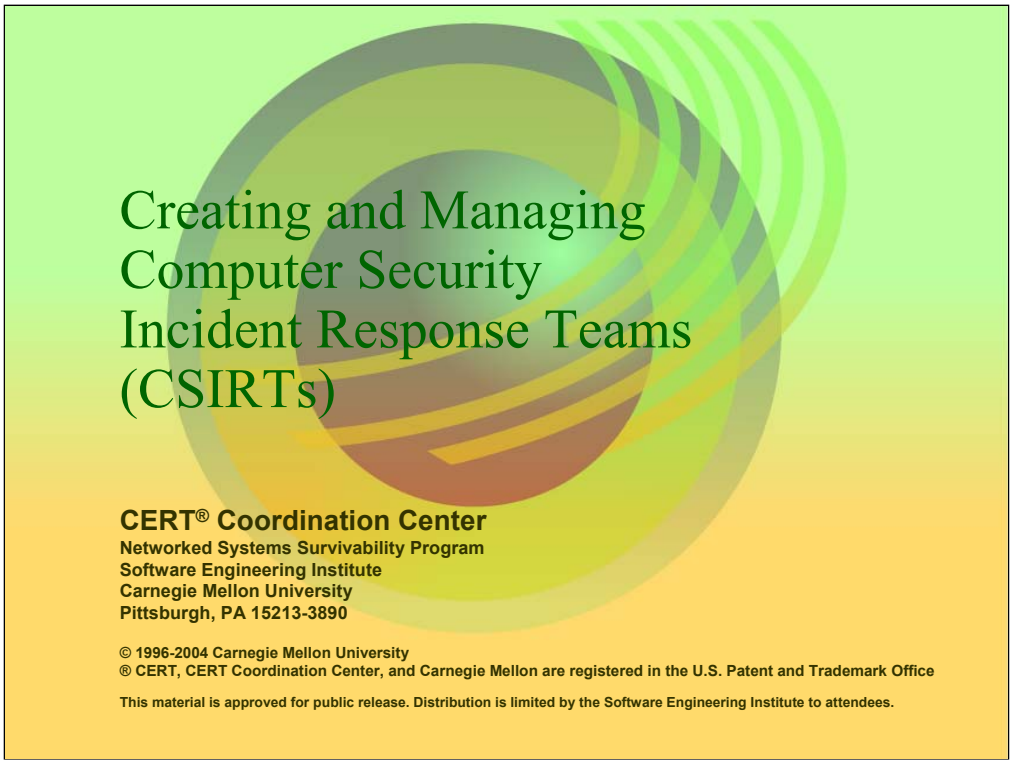


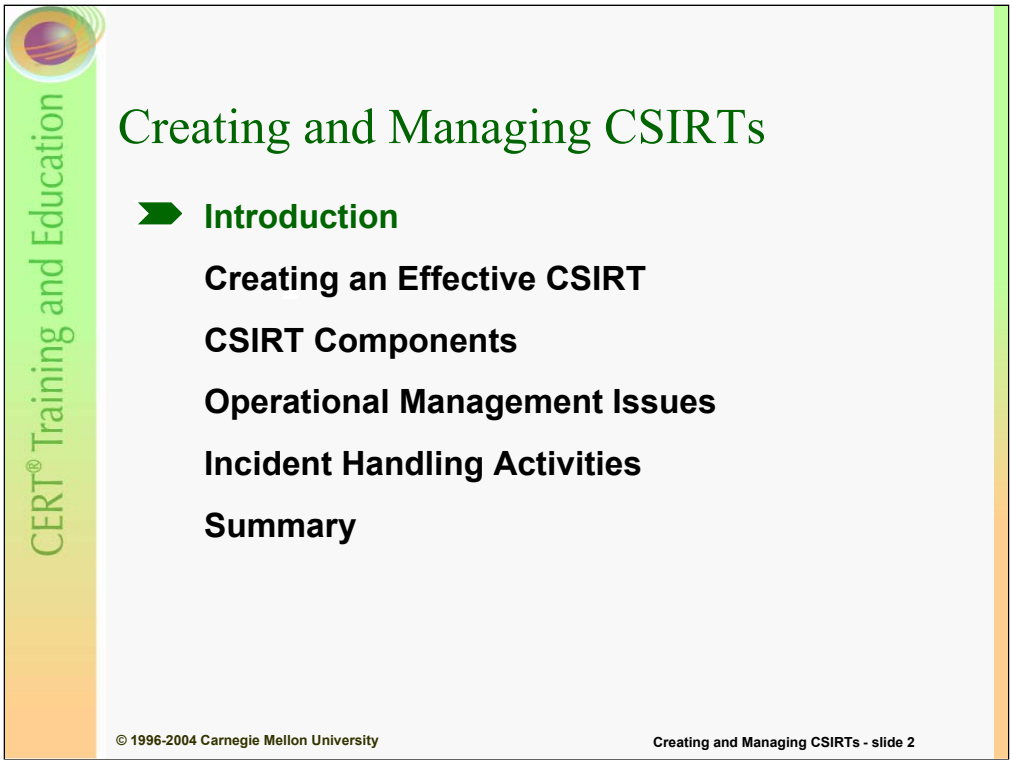
The CERT® Coordination Center (CERT/CC) was created in November 1988 by the Defense Advanced Research Projects Agency (DARPA) in the aftermath of an Internet Worm incident.

The CERT/CC is located at Carnegie Mellon University's Software Engineering Institute (SEI). The SEI is a federally funded research and development center (FFRDC) sponsored by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics [OUSD (AT&L)].

The mission of the CERT/CC is to

- act as a coordination center,
- foster collaboration across the network community to achieve effective incident response,
- assist other organizations in forming response teams, and
- conduct research and analysis of incident trends.

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).



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

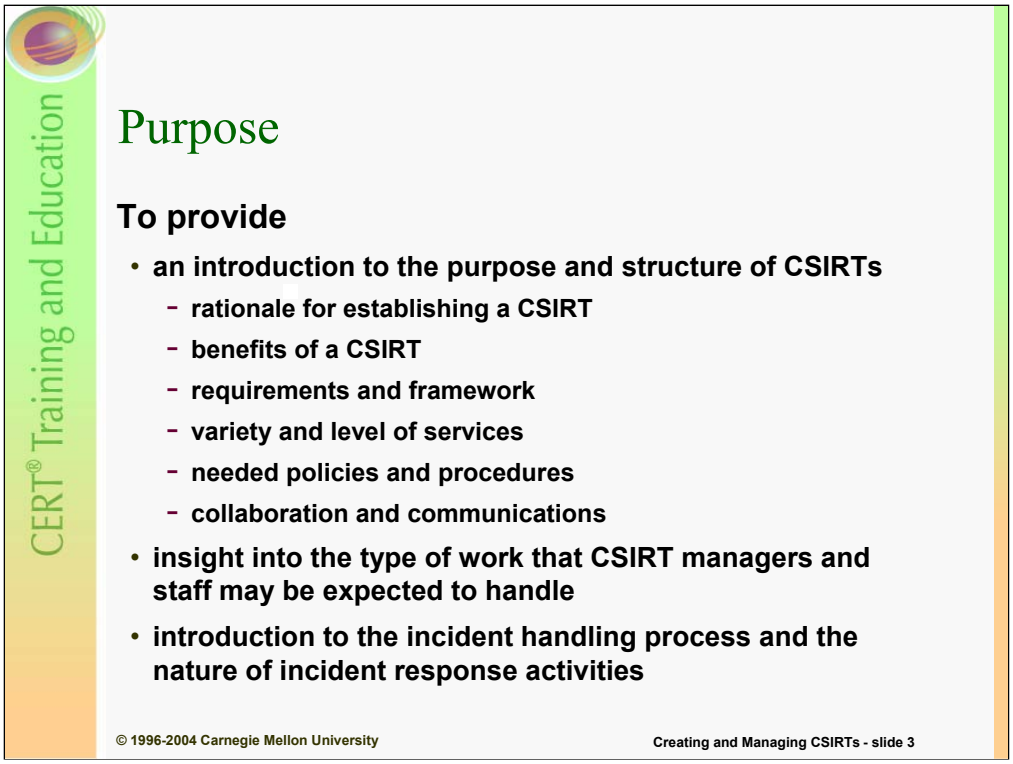
CSIRT Components
- Constituency
- Mission
- Funding
- Organizational Issues
- Services
- Policies and Procedures
- Resources

Operational Management Issues
- CSIRT Staffing Issues
- Managing CSIRT Infrastructures
- Evaluating the CSIRT's Effectiveness

Incident Handling Activities
- Critical Information
- Triage
- Coordinating Response

Summary

Presenter:
Mark Zajicek
CERT® CSIRT Development Team
Networked Systems Survivability Program
Software Engineering Institute
Carnegie Mellon University



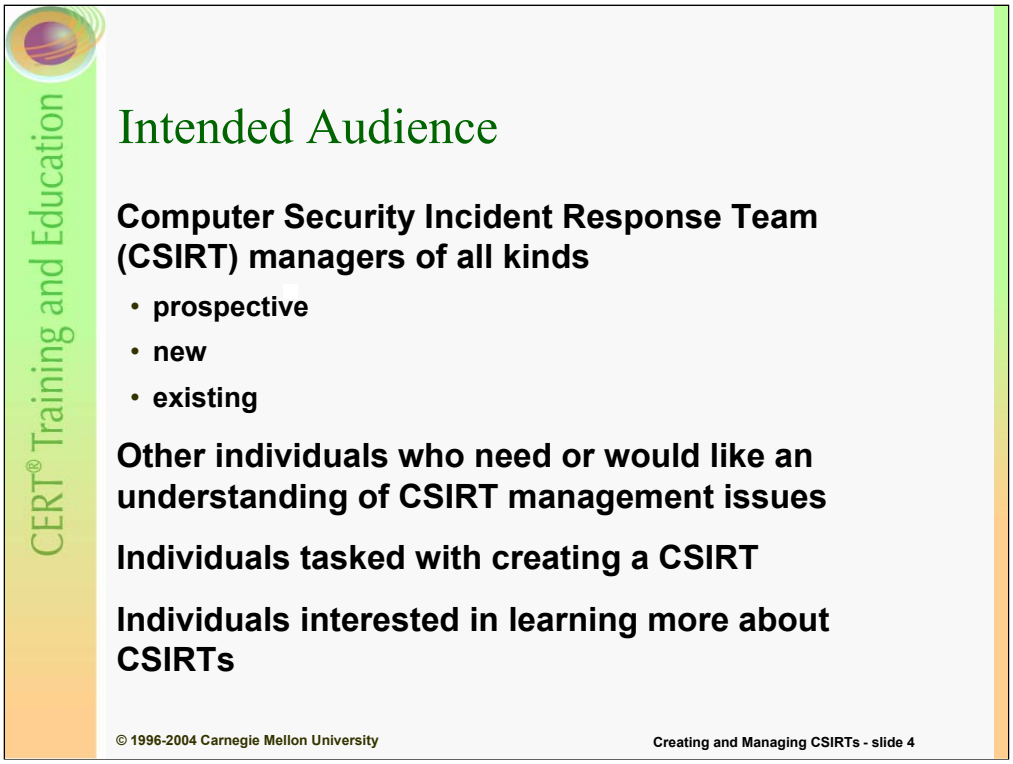
This tutorial presents a high level overview of the management, organizational, and procedural issues involved with creating and operating a Computer Security Incident Response Team (CSIRT).

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 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
- 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

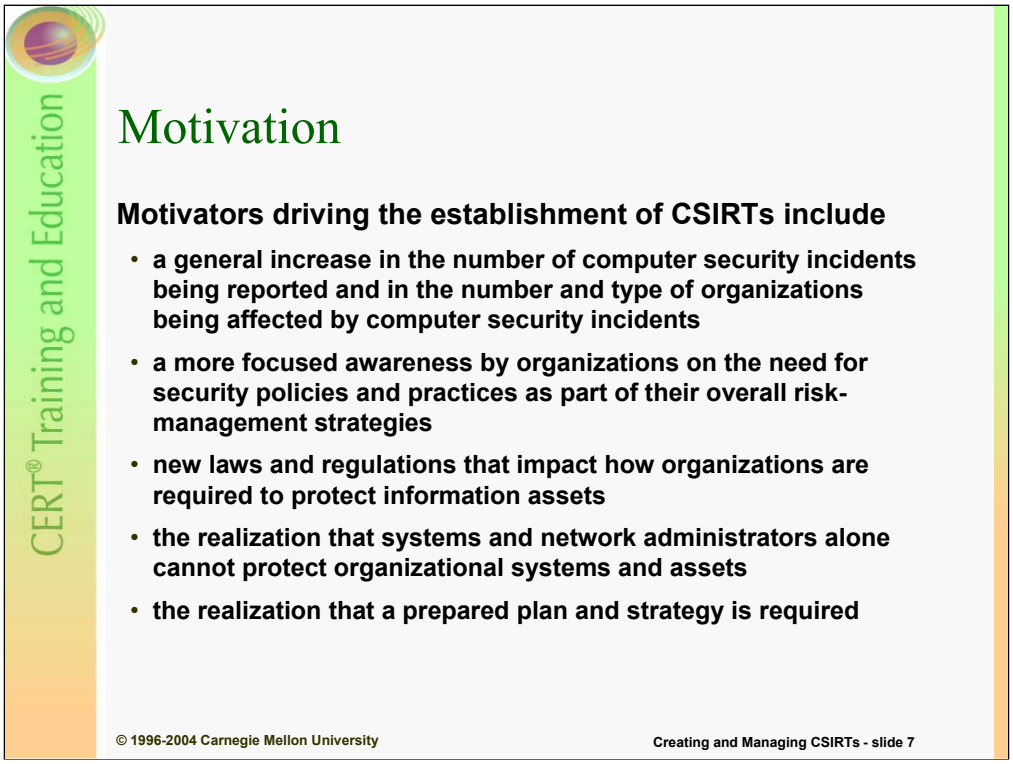
- **what has worked well for the CERT/CC**
- **pitfalls and benefits encountered**

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 Handling Activities
- Summary



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.

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.

Changes in

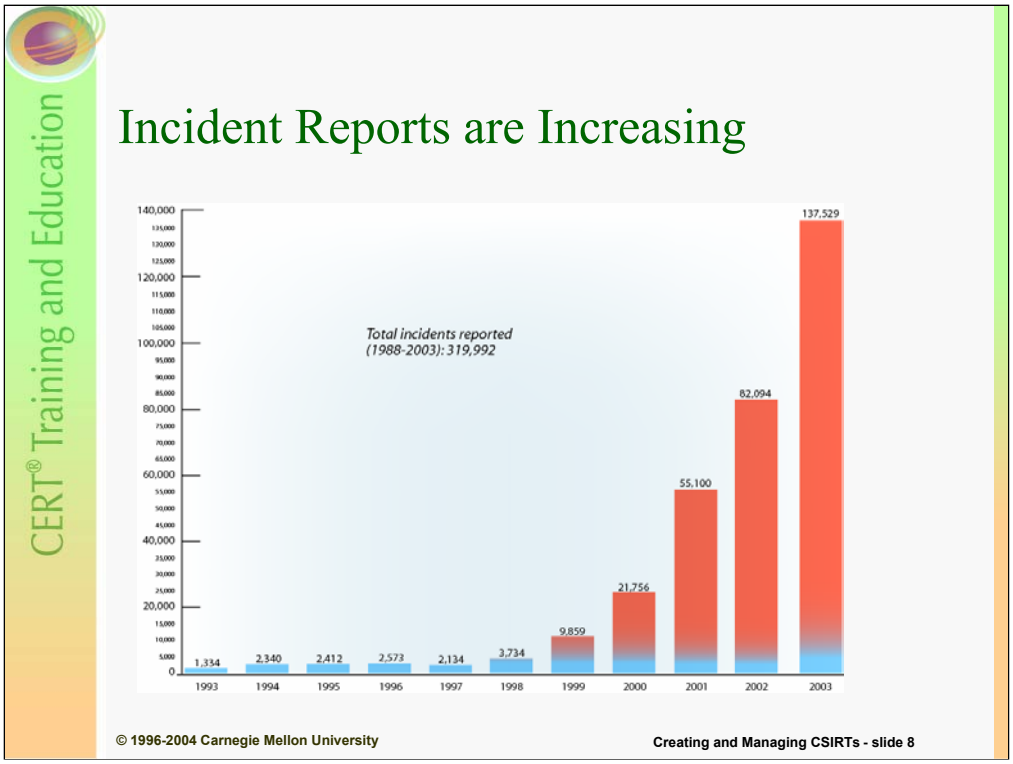
- organizational data protection requirements
- local or national laws
- institutional regulations

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

Some examples in the United States 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.

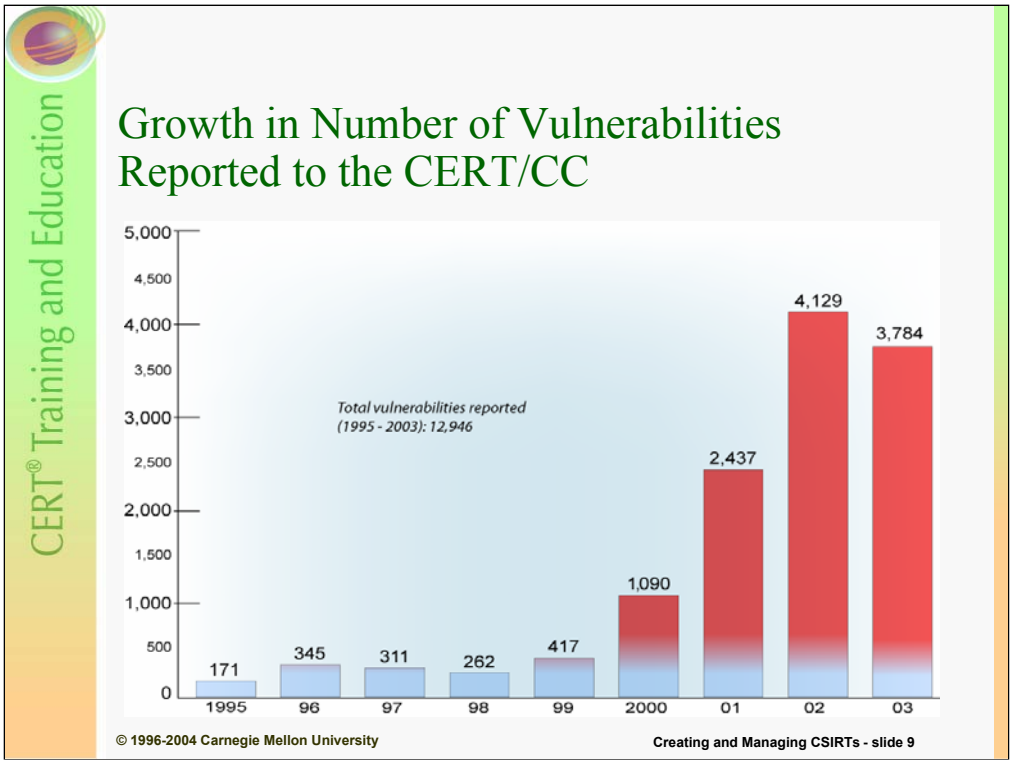
Keeping your organizational information assets secure requires a multi-layered approach. There is no one action or solution that is a panacea.



Above represents reports submitted to the CERT Coordination Center (CERT/CC).

What the Internet community is facing in terms of Internet security in the next few years can be summarized in the following statements:

- the number of companies and users of the Internet is increasing
- the vendor product development and testing cycle is decreasing
- the complexity of protocols and applications run on clients and servers attached to the Internet is increasing
- the complexity of the Internet as a network is increasing
- the information infrastructure has many fundamental security design problems that cannot be quickly addressed
- the expertise of intruders is increasing
- the sophistication of attacks, intruder tools, and toolkits is increasing
- the number of computer security intrusions is increasing
- the effectiveness of intruders is increasing (knowledge is being passed to less knowledgeable intruders thus making them effective)
- the number of people with security knowledge and expertise is increasing, but at a significantly smaller rate than the increase in the number of Internet users
- the number of security tools available is increasing, but not necessarily as fast as the complexity of software, systems and networks
- the number of incident response teams is increasing, but the ratio of incident response personnel to Internet users is decreasing

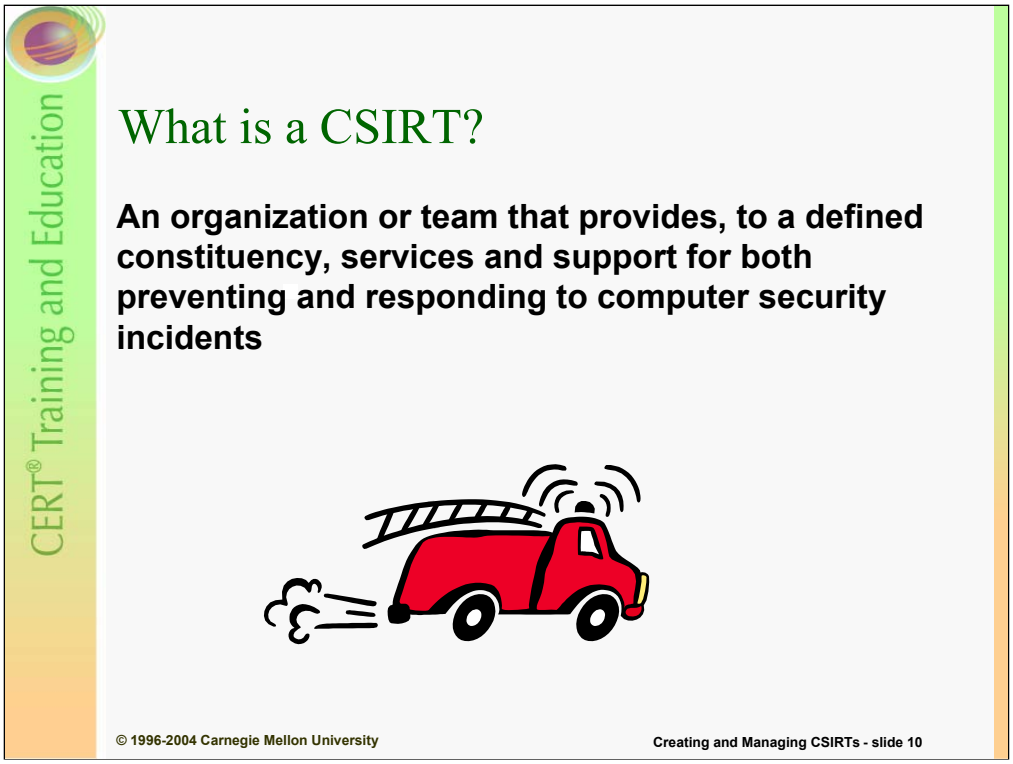


Vulnerability: a set of conditions in a software system that allows an intruder to violate an implicit or explicit security policy.

Examples include

- phf (remote command execution as user "nobody")
- rpc.ttdbserverd (remote command execution as root)
- world-writeable password file (modification of system-critical data)
- default password (remote command execution or other access)
- denial of service problems that degrade service
- smurf (denial of service by flooding a network)
- buffer overflows in software or protocols (BIND, sendmail, FTP, TCP, etc.)

It's also important to recognized that the time from vulnerability discovery to exploitation is getting shorter and shorter: weeks -> days -> hours -> minutes.



Keeping your organizational information assets secure requires a multi-layered approach. There is no one action or solution that is a panacea. Creating a CSIRT is one layer, along with implementing secure configurations, security awareness training, and external and internal defenses.

Aggressive, coordinated response will continue to be necessary, but we must also move quickly to put other solutions in place to achieve the following:

- higher quality information technology products with security mechanisms that are better matched to the knowledge, skills, and abilities of today's system managers, administrators, and users
- expanded research programs that lead to fundamental advances in computer security
- a larger number of technical specialists who have the skills needed to secure large, complex systems
- increased and ongoing awareness and understanding of cyber-security issues, vulnerabilities, and threats by all stakeholders in cyber space

Much like a fire department, a CSIRT can perform both reactive and proactive services.

A fire department responds to and extinguishes fires. They also proactively provide fire-prevention training, promote the installation of smoke alarms and purchasing of fire escape ladders, and instruct families in the best manner to safely exit a burning building.

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

A variety of acronyms have appeared and are used to represent different response teams. Here are a few examples:

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CSIRC	Computer Security Incident Response Capability
CIRT	Computer Incident Response Team
CIRC	Computer Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

CERT® Training and Education

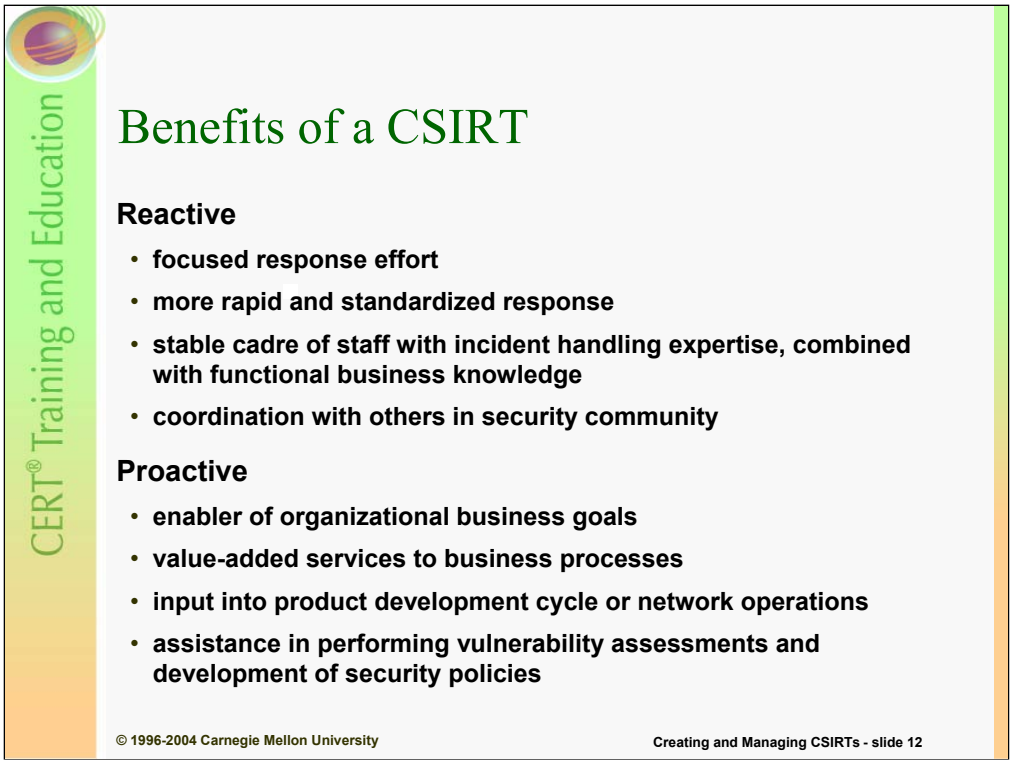
Process versus Technology

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

It is the development of a plan of action.

It is the establishment of processes for

- **notification and communication**
- **collaboration and coordination**
- **analysis and response**



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.

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 understand 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**
- **assists the organizational constituency and general computing community in preventing and handling computer security incidents**
- **shares information and lessons learned with other response teams and other appropriate organizations and sites**

No single team can be everything to everyone!

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

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

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

CERT® Training and Education

General Categories of CSIRTs

Internal CSIRT

- **educational**
- **governmental**
- **commercial**

Coordination Centers

- **country**
- **state**
- **region**

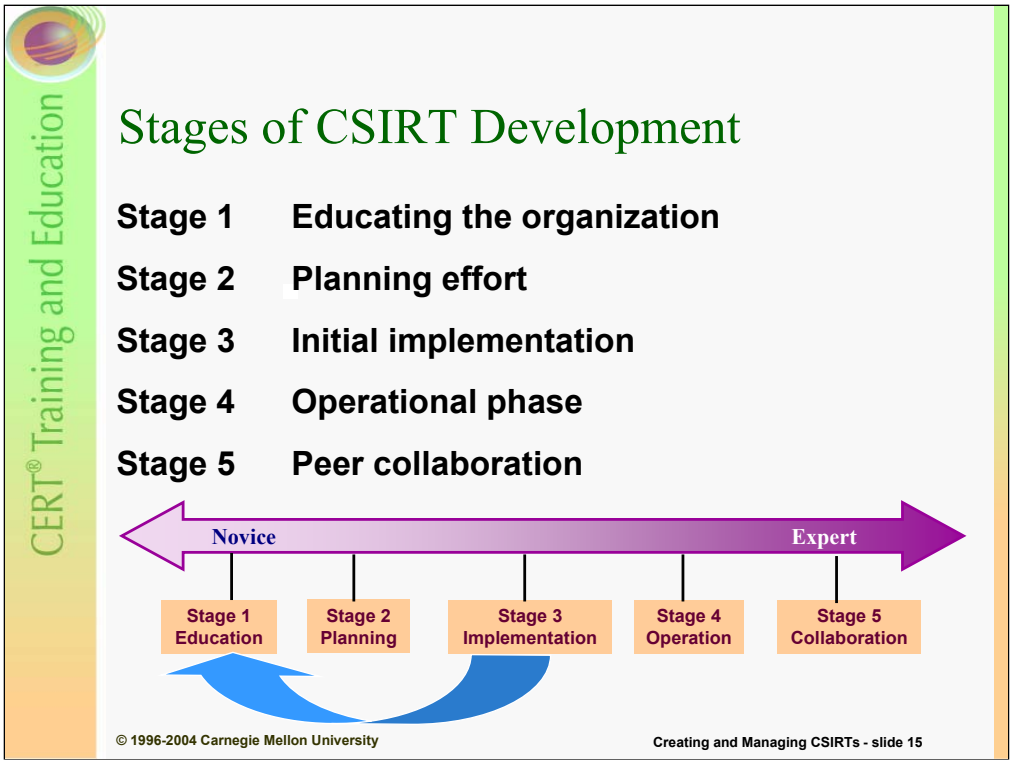
Analysis Centers

Vendor

Incident Response Provider

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, 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).



This slide represents the stages in a CSIRT's development according to the CERT 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. To begin operation it should 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

To be effective, a CSIRT requires four basic elements.

- **an operational framework**
- **a service and policy framework**
- **a quality assurance framework**
- **the capability to adapt to a changing environment and changing threat profiles**

Operational framework

- clear mission
- defined constituency
- organizational home
- formal relationship to other organizational teams

Service and policy framework

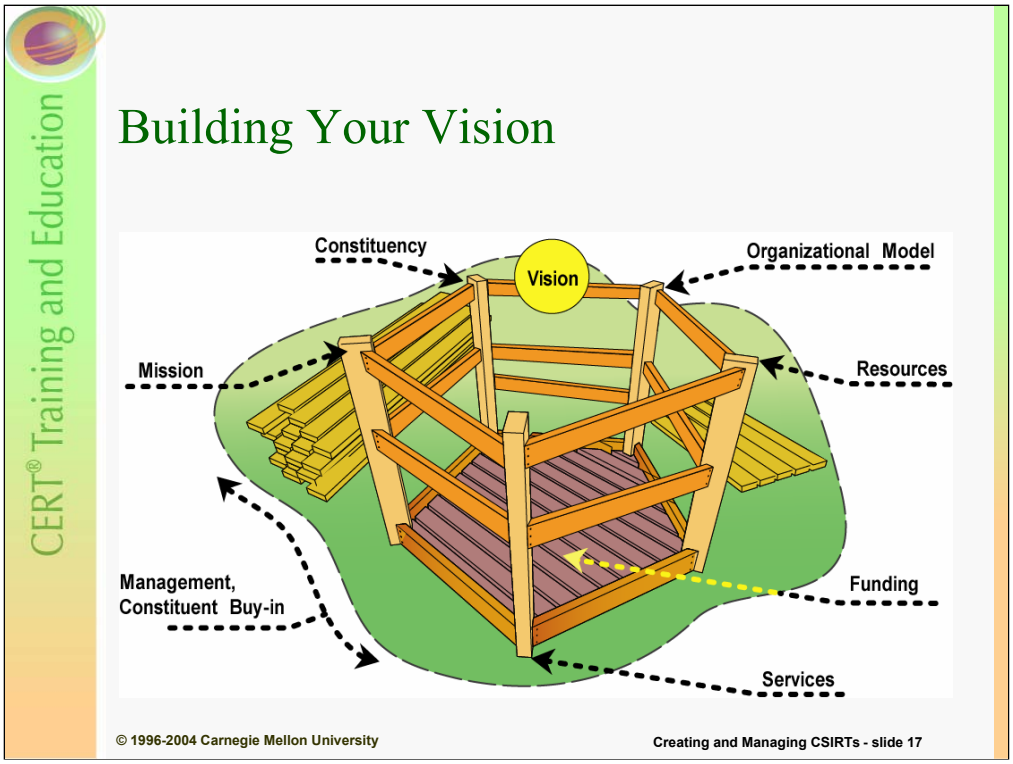
- defined services
- defined information flow
- defined process for collecting, recording, tracking, and archiving information
- clear, comprehensive organization-wide policies

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 keep up with changing technologies
- ability to adapt to real-time threats and future emerging threats
- legal expertise and support



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 will need to take all of these components into consideration and attempt to find the right balance between them.

CERT® Training and Education

What Needs to Be Done?

Establish a response plan.

- integrated into the existing processes and organizational structures
- to strengthen and improve the capability of the constituency to effectively manage computer security events
- as part of an overall strategy to protect and secure critical business functions and assets

Train staff to be able to identify both

- the scope and impact of threats to business functions
- the appropriate mitigation and recovery solutions

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

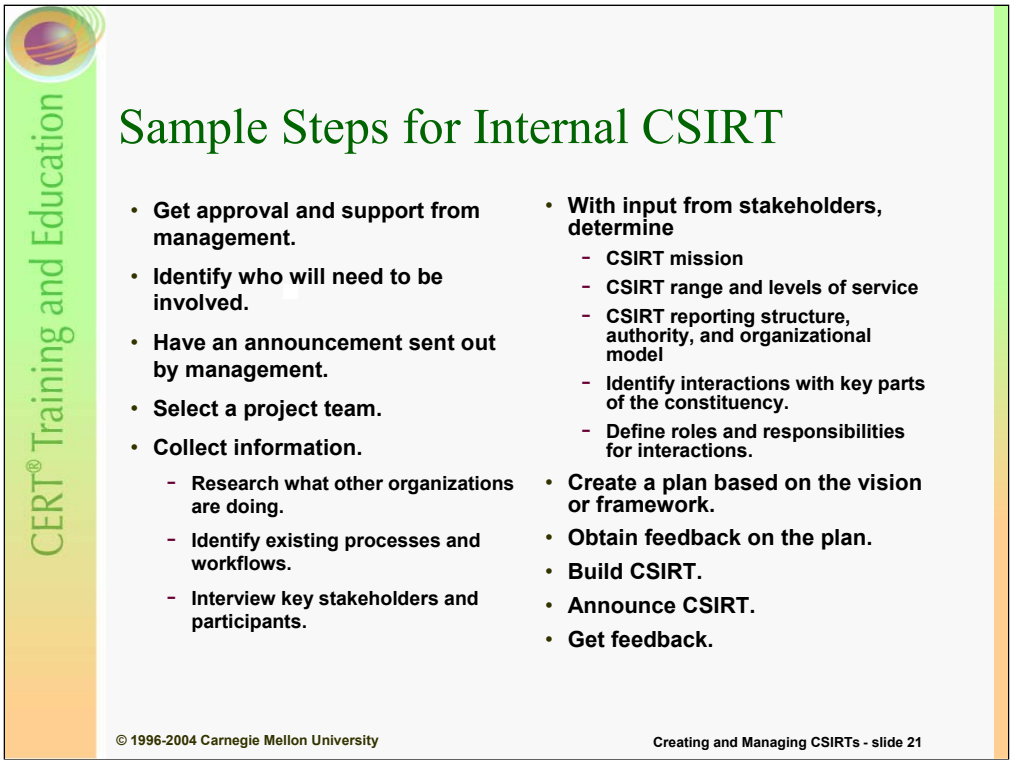
Basic Implementation Steps

- 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.

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.



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?**

As you begin to establish your vision and framework, look to other teams and 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 that people may have written about Incident Handling or CSIRTs.

An initial list of resources can be found at the CERT CSIRT Development Web page: http://www.cert.org/csirts/resources.html

CERT® Training and Education

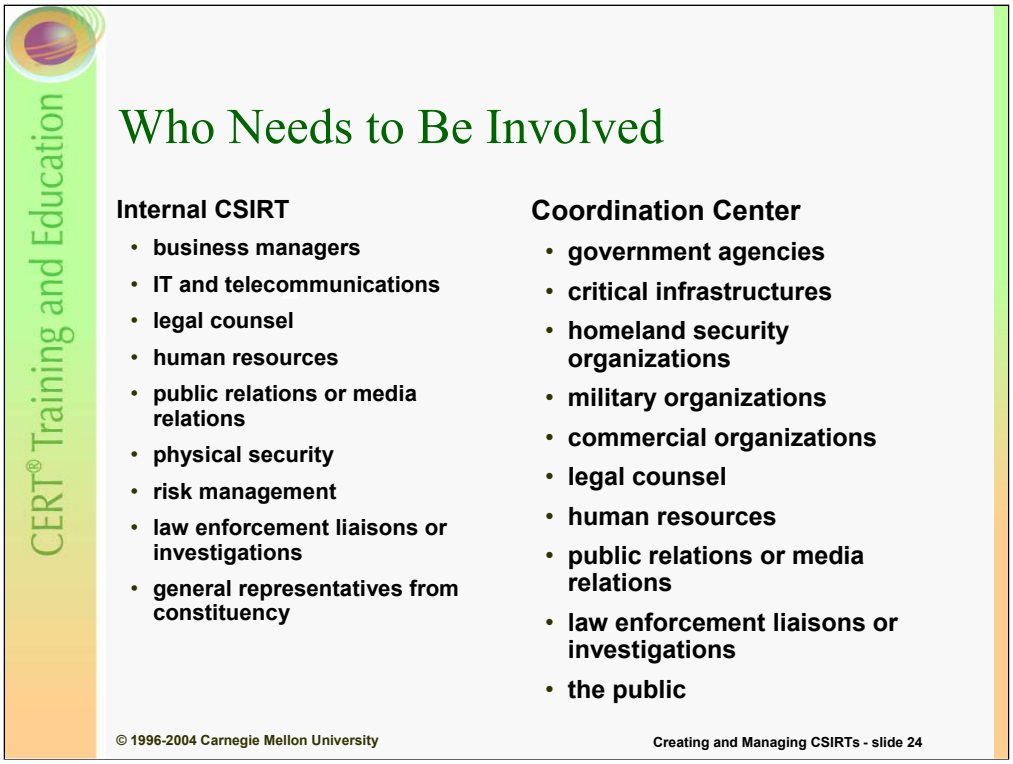
Existing Resources That May Help

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.



You can not understand the nature of the security risks without gathering information throughout your constituency and parent organization. Talk to

- 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 vice-versa?
- 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 your team will 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.

CERT® Training and Education

Where Do You Begin?

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

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

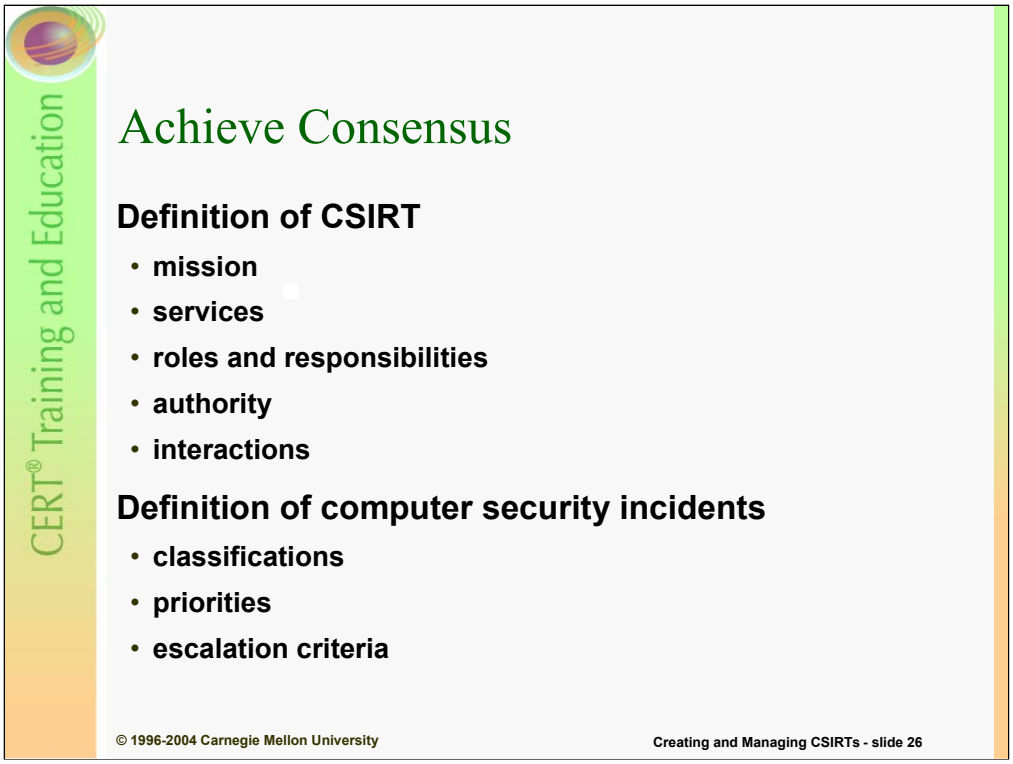
Brainstorm and discuss – design the workflow.

- **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.**

Is there already a tracking system that you must integrate with?



What is a computer security incident?

General definitions might include

- Any real or suspected adverse event in relation to the security of computer systems or computer networks.
- The act of violating an explicit or implied security policy.

A CSIRT requires established criteria that defines not only what constitutes a computer security incident but also how it should be handled.

- This definition can be defined in a security policy; it should also be defined in your incident reporting guidelines.
- The critical assets of your organization that must be protected should also be defined.

Examples of computer security incidents include

- failed or successful attempts to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to systems without the owner's consent
- the occurrence of computer viruses
- probes or scans for vulnerabilities via the network to a range of computer systems

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**

Organizational battles

Taking on too many services

Unrealistic expectations or perceptions

Lack of time, staff, and funding

CERT® Training and Education

Creating and Managing CSIRTs

- Introduction
- Creating an Effective CSIRT
- **CSIRT Components**
- Operational Management Issues
- Incident Handling Activities
- Summary

CERT® Training and Education

CSIRT Components

- **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 project.

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?

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.

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**

Some basic questions?

- **Is the main purpose of the CSIRT to recover systems or to collect evidence?**
- **Will the CSIRT perform**
  - **forensics analysis tasks?**
  - **IDS or firewall maintenance?**

RFC 2350, Expectations for Computer Security Incident Response, is an Internet Best Current Practice (BCP) 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]

The URL for this RFC is
http://www.ietf.org/rfc/rfc2350.txt

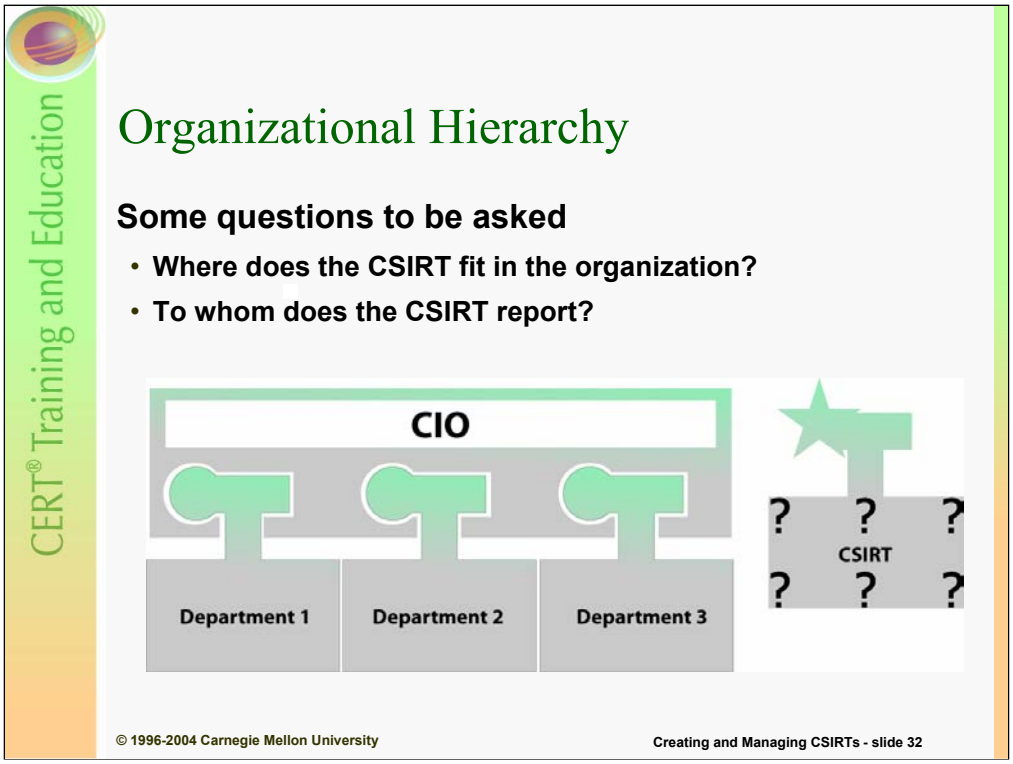
According to the *Handbook for Computer Security Incident Response Teams (CSIRTs)*, Second edition (pages 10-11), your mission statement should

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

Issues to be addressed may include

- How do you deal with the public perception of CSIRTs as "cybercops"?
- What should be done if your mission overlaps the mission of another part of the organization?

http://www.cert.org/archive/pdf/csirt-handbook.pdf



The first 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.

The CERT/CC conducted an informal survey of 14 CSIRTs - the majority of them indicated that their incident handling capability was located in the Information Technology (IT) department of the parent company. We do not have information on why that is the case. It could be related to issues of convenience or expertise. It could also be a strategic decision.

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.

CERT® Training and Education

CSIRT Interaction With Enterprise

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?

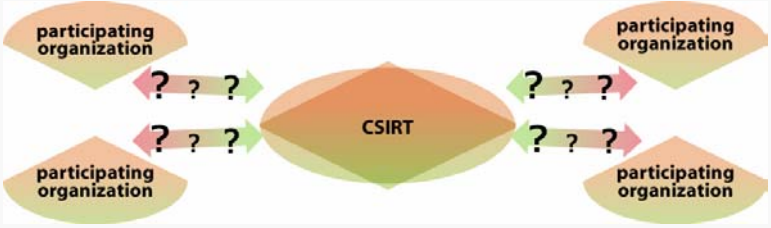
How will the CSIRT make recommendations for changes to internal and external defenses like firewalls or IDS?

CERT® Training and Education

Reporting Structure – National, State, or Coordinating CSIRT

Some questions to be asked

- **Who will host the CSIRT?**
- **Who will be supported by the CSIRT?**
- **Who will report incidents and information to the CSIRT?**
- **Who will receive notification and information from CSIRT?**



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?

CERT® Training and Education

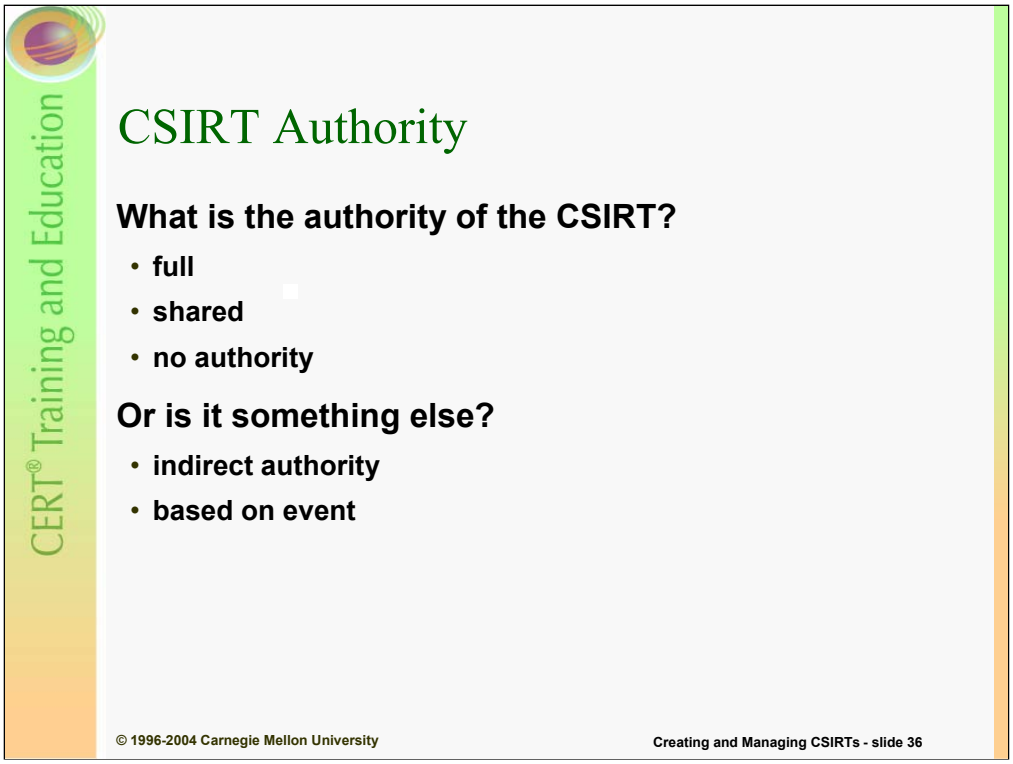
CSIRT Interaction with Constituency

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.



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* (Second edition, 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 (mentioned on page 15 of the *Handbook for CSIRTs [Second edition]*) 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.

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

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

How Big Should Your CSIRT Be?

Size will be different, based on missions, goals, services, experience, workload, and costs.

Ensure that you don't have a single point of failure.

Ensure that your CSIRT staff are cross-trained.

Understand that estimates by other organizations may not fit your situation.

There is no simple answer to this question. Different CSIRTs have different staffing levels that fit their models. Currently there is no true scientific study, just some anecdotal information.

Quantifying this type of effort and cost is very difficult. You must base your decision on the workload and resources you have. Always remember that you never want one point of failure, so one person devoted to incident response will never be enough.

CERT® Training and Education

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 have 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, Compaq, etc. are members of FIRST

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

Combination of the above
- CERT/CC is funded by government and private sponsorship

CERT® Training and Education

How Much Will It Cost?

This will depend on the CSIRT structure and services.

Think about both short-term and long-term costs.

- **short-term start up costs: staff, equipment, infrastructure**
- **base funding to support your initial services and activities**
- **long-term costs necessary to grow**

Primary cost will be for

- **staff and training**
- **equipment, infrastructure, and incident handling tools**
- **physical space and secure access**

Do you know what your budget will need to be?

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.

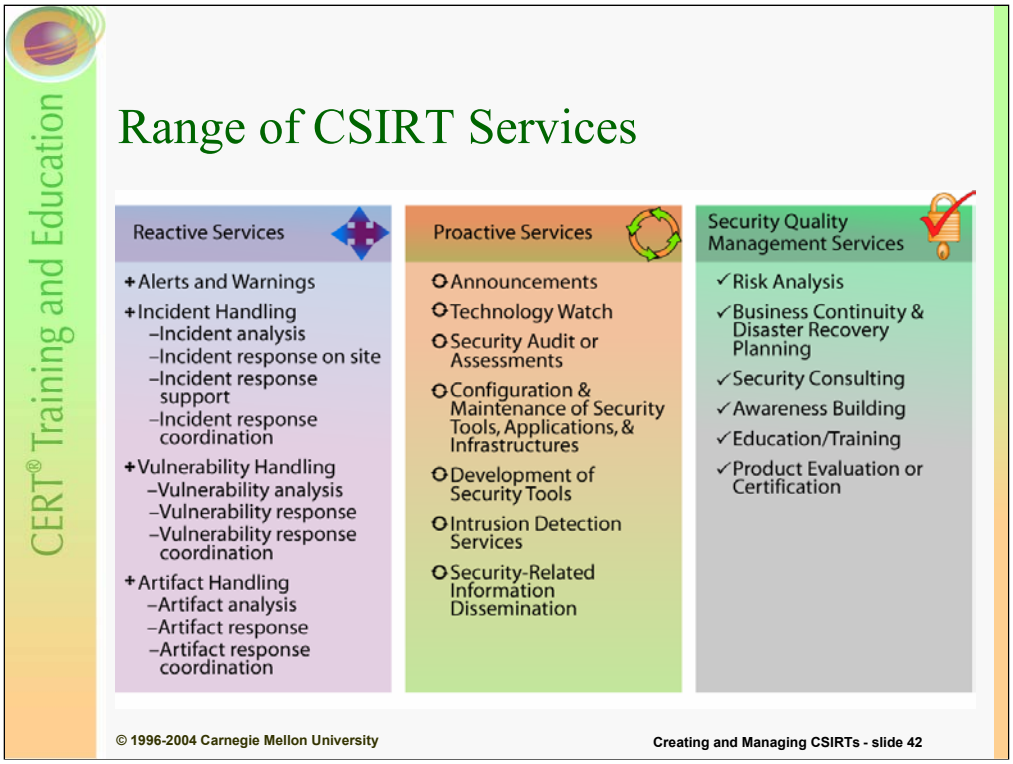
CERT® Training and Education

Some Basic Costs

Costs may include

- **incident reporting and tracking system**
- **communications mechanisms**
  - **hotline or helpdesk**
  - **web site and/or ftp site**
  - **mailing distribution lists**
  - **cell phones and pagers**
- **secure communications mechanisms**
  - **PGP keys or digital certificates for signing CSIRT documents and mailings**
  - **secure phones**
  - **intranets or extranets**
- **secured access to CSIRT facilities**

We will discuss these in more depth in later sections.



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 the article CSIRT services at

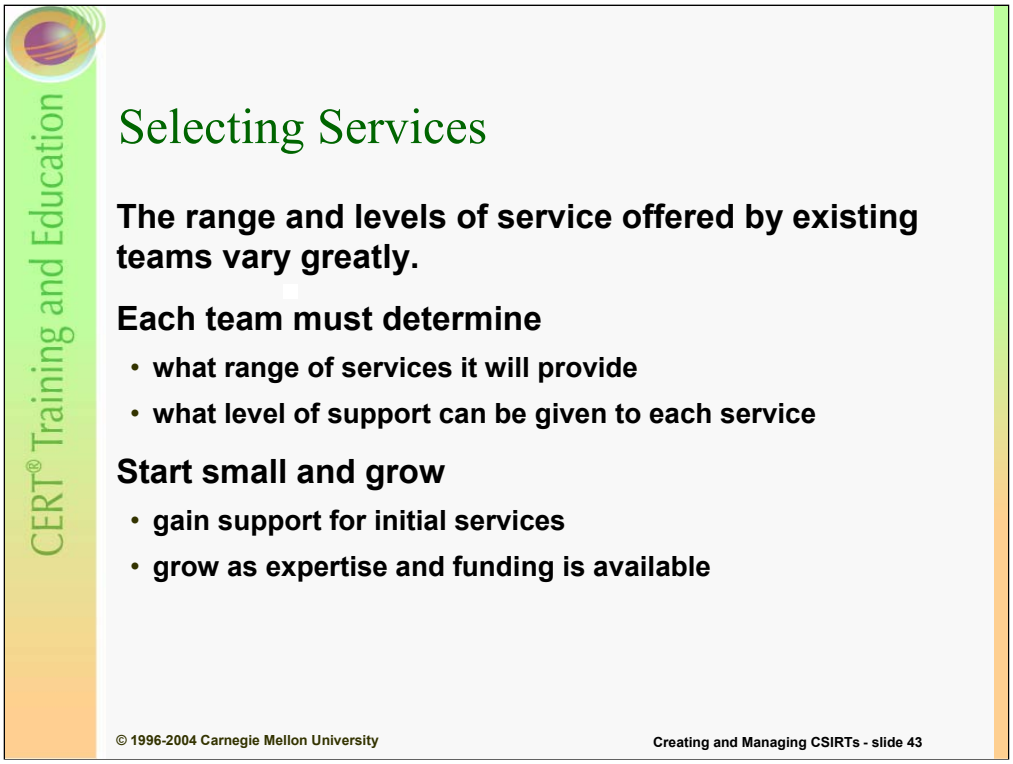
http://www.cert.org/csirts/services.html

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.

Depending on the mission or goals, teams may perform some (or all) of these services.

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

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



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).

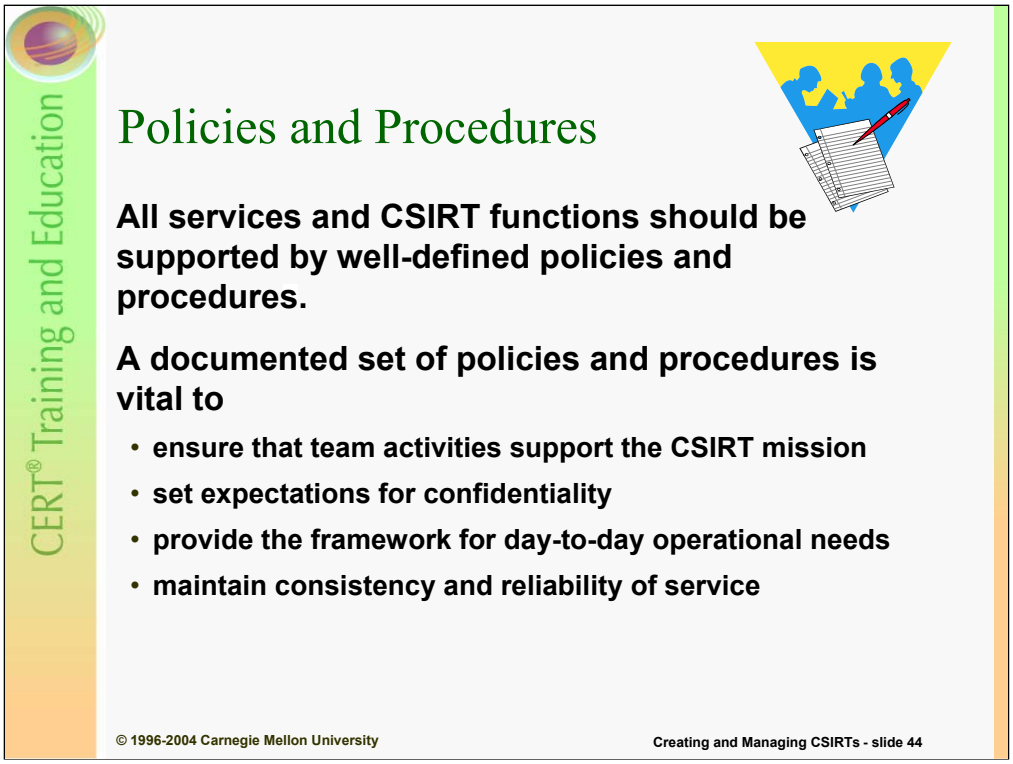
It is recommended that a CSIRT start with a small subset of services, gain acceptance of the CSIRT by the organization through quality service and response, then begin to develop and expand the capabilities of the CSIRT as they are needed and can be effectively supported.

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



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

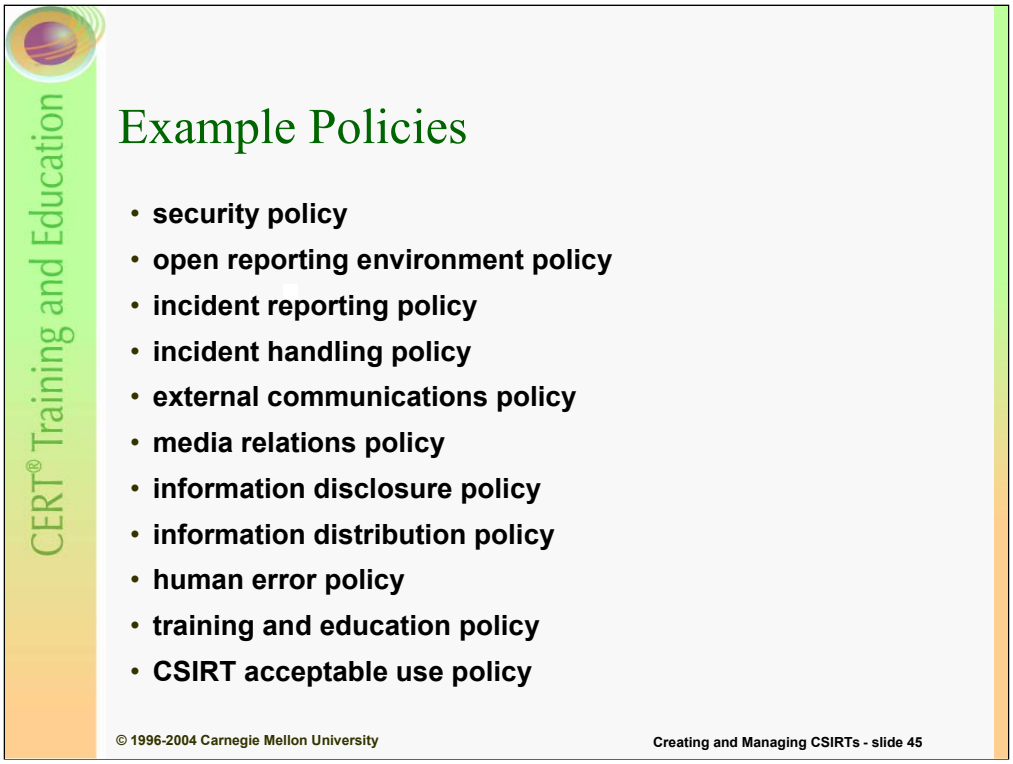
Well-defined policies and procedures offer guidance for CSIRT staff operations.

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.



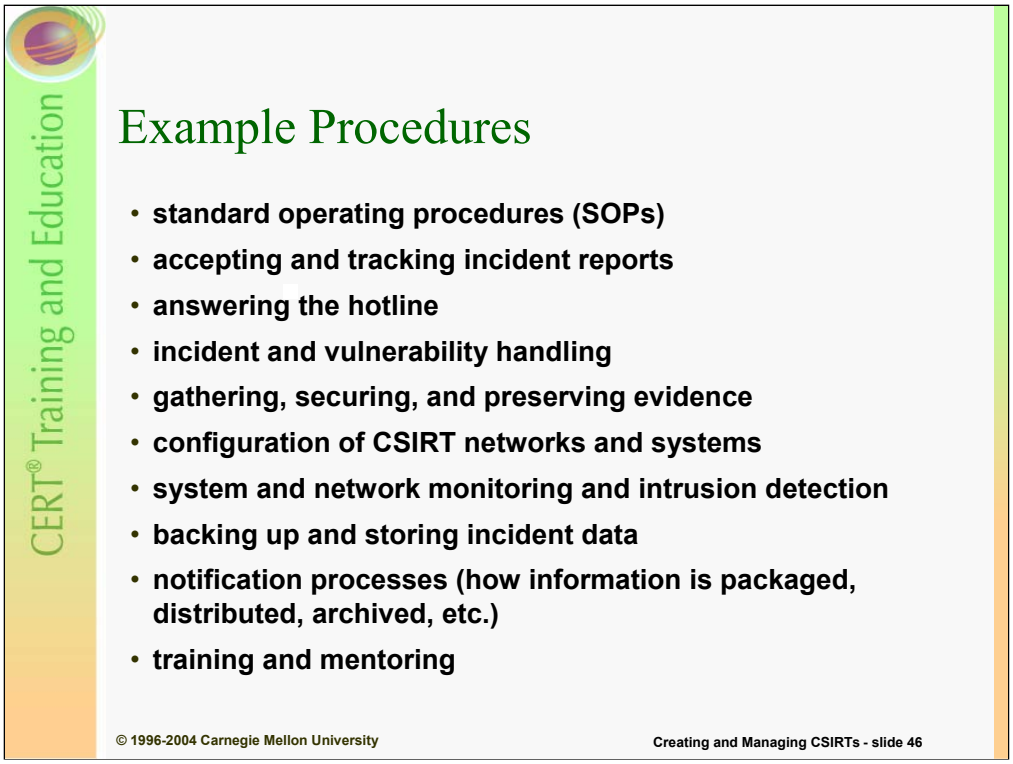
Policies must be clearly understood so that staff can correctly implement procedures and enact their responsibilities.

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.



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.

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.

CERT® Training and Education

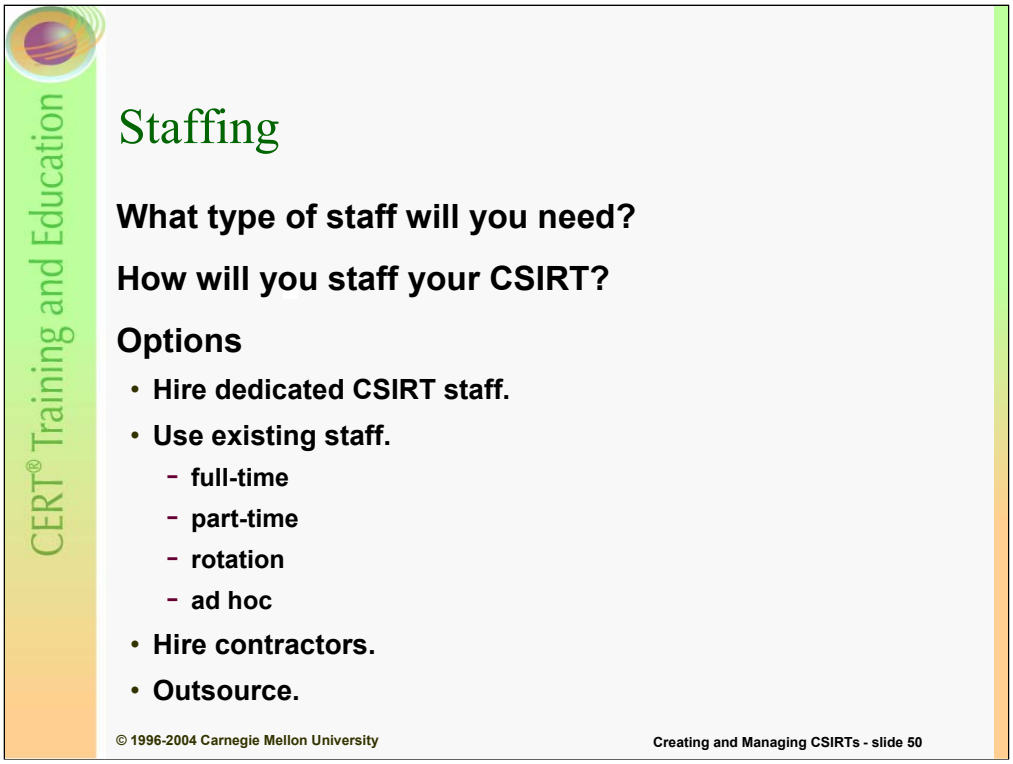
Creating and Managing CSIRTs

- Introduction
- Creating an Effective CSIRT
- CSIRT Components
- **Operational Management Issues**
- Incident Handling Activities
- Summary

CERT® Training and Education

Operational Management Issues

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



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

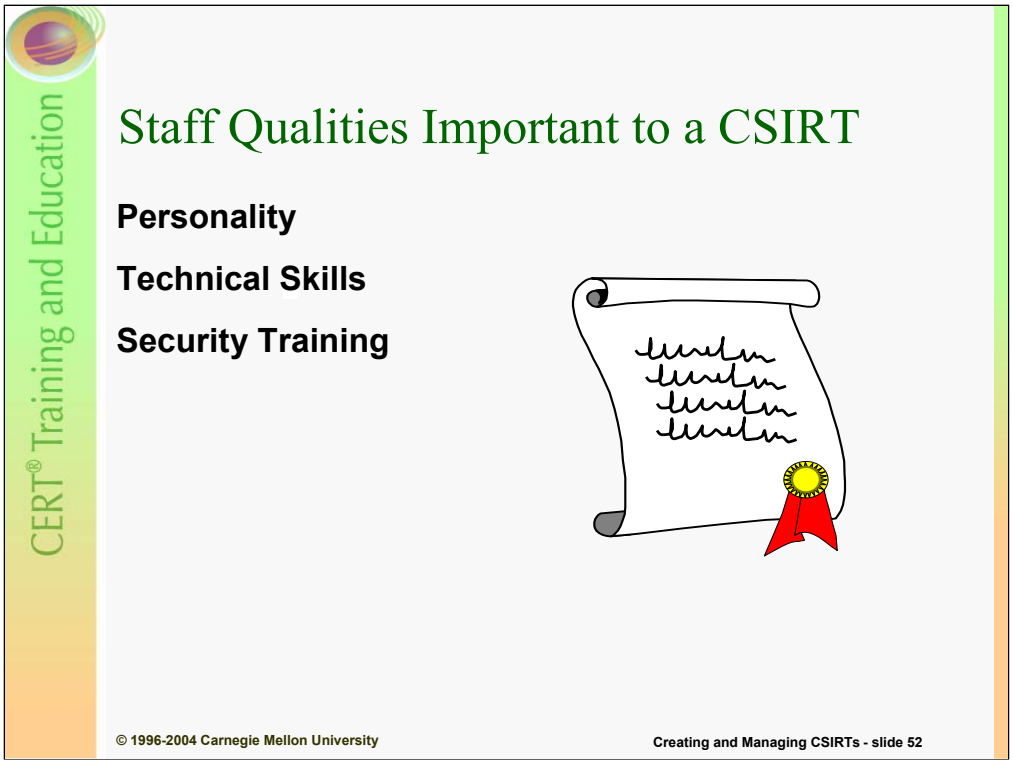
- manager or team lead
- assistant managers, supervisors, or group leaders
- hotline, help desk, or triage staff
- incident handlers
- vulnerability handlers
- artifact analysis staff
- forensic analysts
- platform specialists
- trainers
- technology watch

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.



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.

Personality

- people skills
- communication skills

Technical Skills

- system and network administration experience
- platform expertise: UNIX/Linux, Windows, Mac
- basic understanding of Internet protocols
- programming experience

Security Training

- incident handling experience
- problem solving abilities
- basic understanding of common computer attacks and vulnerabilities

Be aware of

- any requirements you might have regarding obtaining security clearances
- the need for service level agreements and data protection agreements with contractors and managed service providers
- You may want to review the CERT/CC Security Improvement Module, *Outsourcing Managed Security Services*
  - http://www.cert.org/security-improvement/modules/omss/ http://www.cert.org/security-improvement/modules/omss/omss.pdf

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**
  - **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/

Other resources

- SAGE/SANS/BigAdmin Annual Salary Survey
  http://portal.sans.org/index.php?salarysurvey02=Y

CERT® Training and Education

Operational Management Issues

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

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.

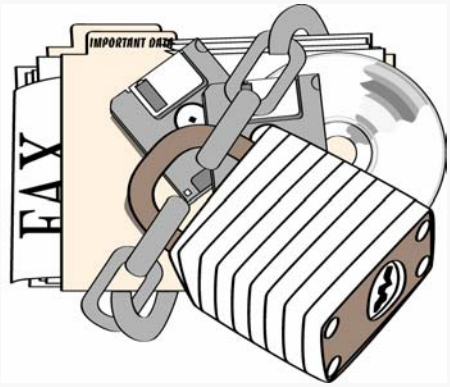
http://www.cert.org/octave/

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**



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**

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**

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

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

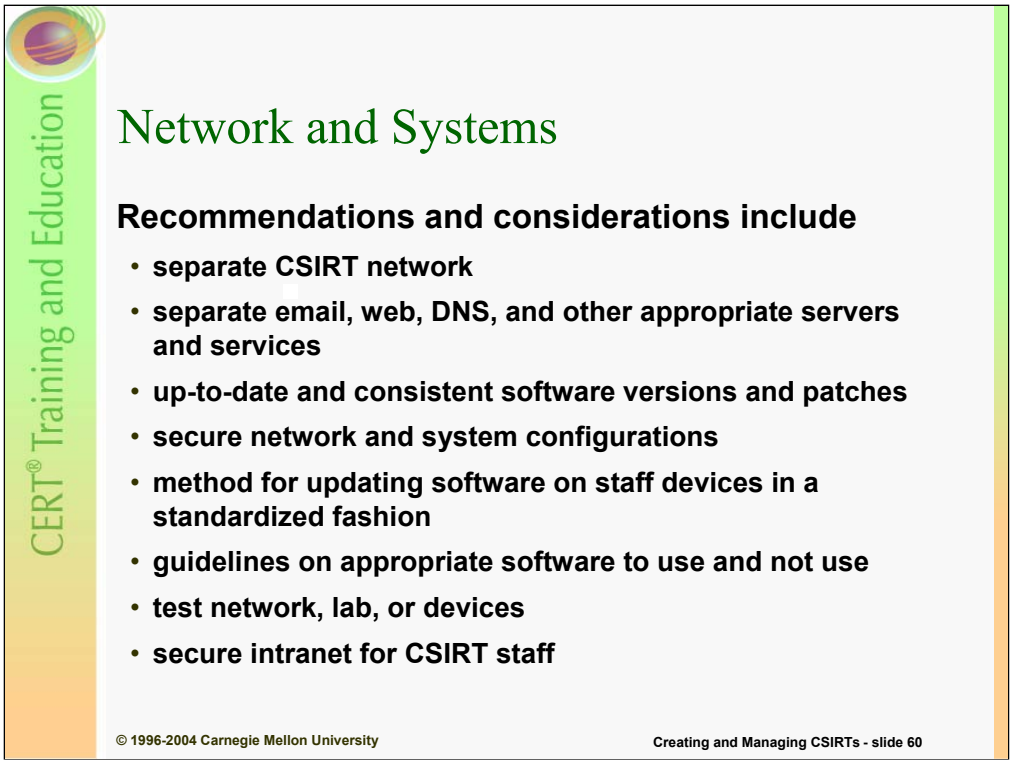
- Locate printers that are used to print sensitive data in a secure area.
- Store output from printers in a secure location.
- Remember: FAX machines are printers, too.

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?



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?

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

CERT® Training and Education

Data Storage, Analysis, and Tracking

CSIRTs require a robust tracking system for receiving, storing, and querying information.

This system may include or require

- **trouble ticket or help desk system**
- **relational database**
- **query and analysis tools**

How the data will be recorded and stored will depend on the ultimate use of the data. Some thought should go into determing this before the storage, tracking,and analysis tools are developed.

You may require more than one system or an integrated system depending on your services, such as

- incident handling
- vulnerability handling
- artifact analysis

The CERT/CC currently has separate incident and vulnerability reporting and tracking systems. Our Artifact Analysis team is also currently developing a database to store, track, and query artifacts.

CERT® Training and Education

Necessary Tools

Tools are needed for

- **storing, analyzing, and tracking CSIRT data**
- **analyzing logs, files, and artifacts**
- **identifying addresses and contacts**
- **scanning your systems**
- **connection monitoring**
- **intrusion detection**
- **access control**
- **file integrity checking**
- **encryption/decryption**
- **secure communications**
- **verification**

The next series of slides will provide an overview of some of the types of tools that your staff may need to not only perform day-to-day incident handling work but to also protect CSIRT data and systems.

Inclusion of tools and products in this session does not constitute an endorsement by the CERT/CC.

CERT® Training and Education

Custom Documents

Standardized replies and "technical tips" save time in answering frequently asked questions.

- **reusable text from email messages**
- **interactive reporting forms**
- **pointers to resources available on your web site**
  - **"how-to" documents**
  - **in-house tutorials or training**
  - **frequently asked questions (FAQs)**
  - **current activity or "what's new"**
  - **custom or personalized web pages**
  - **advisories or alerts**
  - **incident or vulnerability notes**
  - **other information**

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**

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**

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**

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**

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 Handling Activities**
- Summary

CERT® Training and Education

Incident Handling Activities

Incident Handling Activities

- **Critical Information**
- **Triage**
- **Coordinating Response**

CERT® Training and Education

What Is Incident Handling?

Within the mission and scope of your CSIRT, incident handling includes the complete process of

- **receiving requests for service and incident reports from your constituency members**
- **analyzing requests and reports**
- **responding appropriately to those requests**

It also includes the process of tracking and recording your incident handling activities.

Incident response can take many forms: on-site response, support, or coordination.

Incident Handling includes three functions: incident reporting, incident analysis, and incident response.

A CSIRT will work with the reporting site to confirm that an incident has occurred.

In determining the magnitude and scope of the incident, consider

- the number of internal and external hosts
- the vulnerabilities or methodology exploited

To protect the evidence, capture a system snapshot for further analysis.

Be sure to communicate the problem and actions taken to

- management
- other response organizations
- your operations group
- all affected sites
- appropriate investigative agency
- CERT/CC

In recovering from incidents

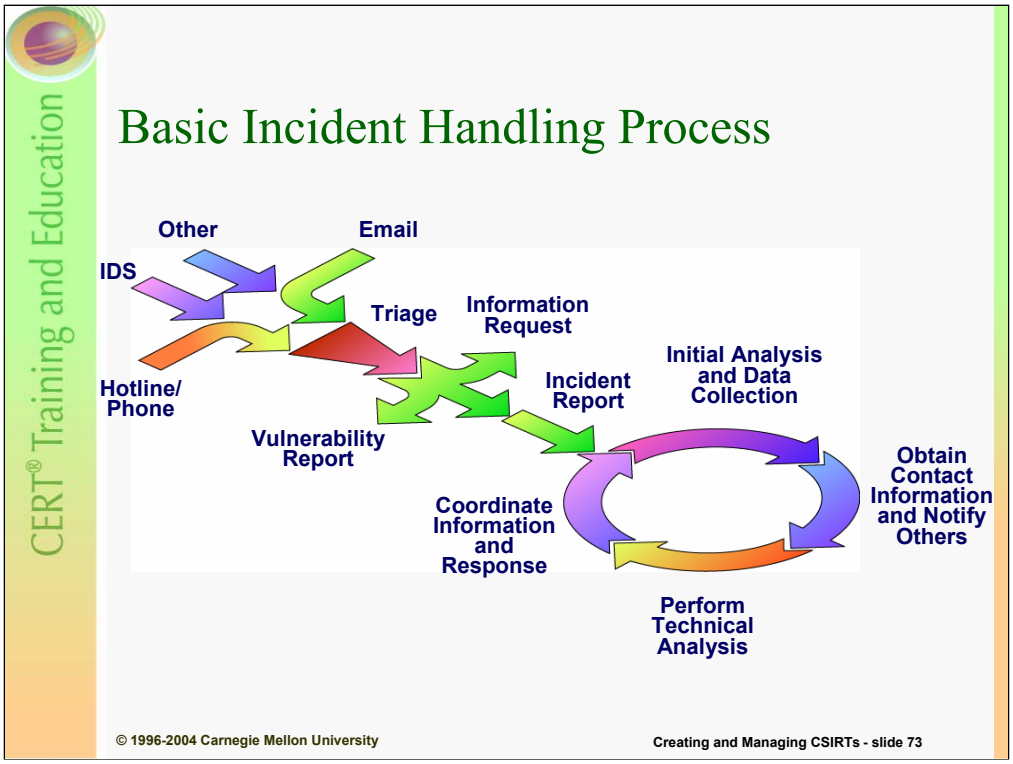
- restore programs and applications from vendor-supplied media
- restore data from periodic backups. Be careful when restoring from backups

During a post-mortem

- review lessons learned
- evaluate procedures

For more information see

http://www.cert.org/tech_tips/win-UNIX-system_compromise.html



The above diagram illustrates an example of how incident reports are received and processed. The life cycle shows the main processes and functions that are performed during the handling of an incident.This diagram is based on the manner in which the CERT/CC handles incidents. Your process may be very different depending on your CSIRT's mission and provided services.

In the above life cycle, reports and requests are received from many different inputs: email, phone calls, intrusion detection system (IDS) alerts or logs, even web-based incident reporting forms.

Once the reports/requests are received, they are recorded and categorized through a process called Triage. This process, like the corresponding process in a hospital, is used to identify urgent requests that need immediate attention and to assign other requests to appropriate staff or organizational groups.

If the report is identified as an incident, it is passed on to the incident handling group for initial review and analysis. This may include more data gathering or even forensics evidence collection. At this point there may be some initial steps taken to contain the incident or backup systems for later analysis.

Based on the scope of the incident, other parties may need to be contacted or involved, such as CSIRT members, platform specialists, system and network administrators, business managers, Internet Service Providers (ISPs), other CSIRTs, victim sites, attacking sites, or law enforcement. Incident handlers must often do some research to obtain the contact information for the involved parties.

Once the incident is understood and mitigation or response strategies are identified through technical analysis, the incident handlers will provide the appropriate assistance to help a site recover. Information, solutions, or alerts may need to be disseminated and response efforts coordinated between involved parties.

CERT® Training and Education

The Life of an Incident Handler -1

Tasks and actions performed by an incident handler

- **analyzing reports to determine**
  - **impact**
  - **scope and magnitude**
  - **involved sites**
  - **methods of attack**
  - **trends in intruder activities**
- **analyzing corresponding logs and files such as**
  - **sniffer, firewall, or router logs**
  - **UNIX syslogs, or Windows auditing logs**
  - **intruder files and artifacts**
  - **exploit scripts**

This slide and the following two slides look at each of the processes and functions in the Incident Handling Life Cycle in more depth.

The bulleted lists describe some of the actions and tasks that may be performed by incident handling staff.

Determining the tasks to be undertaken during incident handling activities will help you identify the tools, skills, and practices that the CSIRT staff will need to do their work.

CERT® Training and Education

The Life of an Incident Handler -2

- monitoring network and system logs
  - intrusion detection systems (IDS)
  - firewall or system accounting
  - output of vulnerability scanners
- providing direct technical assistance through
  - on-site assistance
  - telephone response
  - email response
  - email auto-responder
  - web or hardcopy documents

CERT® Training and Education

The Life of an Incident Handler -3

- **researching involved site or host information to**
  - **identify hostnames and IP addresses**
  - **determine site contact information**
- **coordinating and sharing information**
  - **mailing information to involved sites**
  - **encrypting and decrypting sensitive information**
  - **receiving and storing logs, exploits, and files**
  - **tracking tasks and actions**
  - **facilitating communications and collaborating with other sites, CSIRTs, law enforcement, and management**
  - **contacting vendors**
  - **preparing reports, statistics, and briefings**

CSIRTs may also need to

- prepare for media inquiries
- assess time and resources used and damage incurred
- prepare report(s)
- perform forensics analysis
- support prosecution activity and act as expert witnesses (if appropriate)

CERT® Training and Education

Gathering Critical Information

Incident handlers are very much like detectives: always searching for data.

Identify which information is important to the handling of an incident, so that your CSIRT can try to gather it.

Determine how you are going to capture this information.

- **log sheets**
- **database**
- **email**
- **interactive web forms**

You will also get information from network and system logs and artifacts.

CERT® Training and Education

Critical Information

Information to gather during incident handling

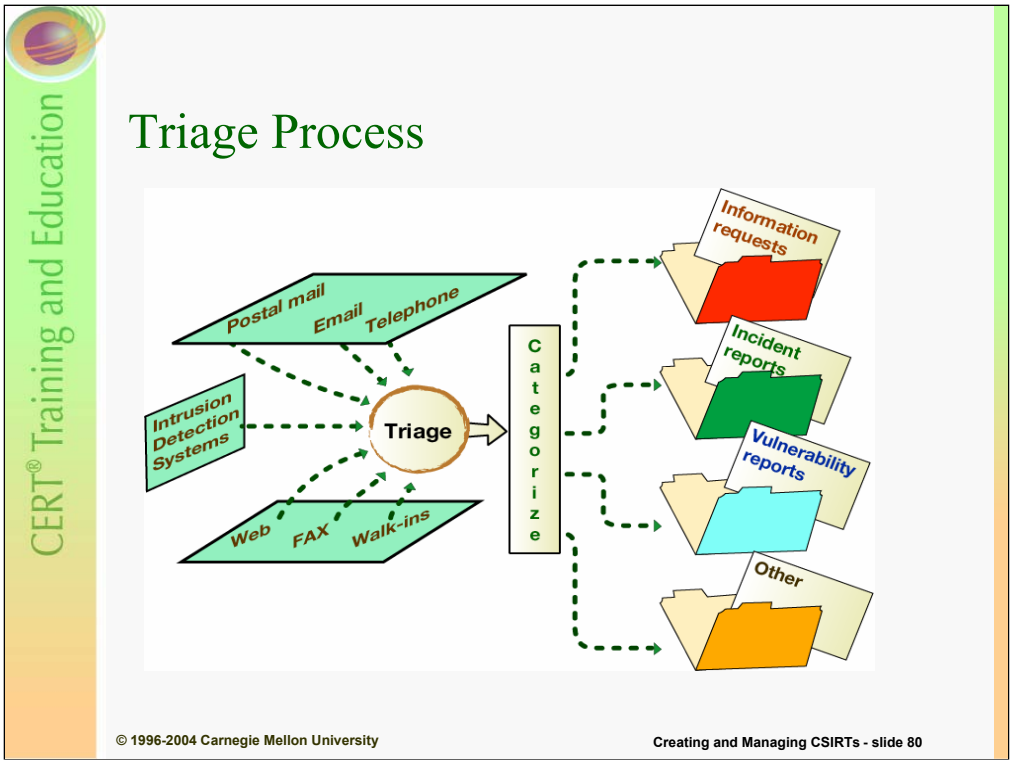
- **Who is involved? What is their contact information?**
- **Whom do they represent?**
- **How are they involved?**
- **What is their role?**
- **What is the nature of the incident?**
- **What is the scope of the incident?**
- **What is the time frame of the report and the reported activity?**
- **What has been done, and who else has been contacted?**
- **What supporting information is available?**

CERT® Training and Education

Incident Handling Activities

Incident Handling Activities

- **Critical Information**
- **Triage**
- **Coordinating Response**



Triage is the

- first step in incident response
- single point of entry for all CSIRT correspondence
- central location for incident reporting
- mechanism and set of tools used to identify, categorize, and assign all incoming correspondence and reports

Information flows into the focal “triage” point. From there it is processed, identified, and categorized to the appropriate service foundation.

All CSIRTs implicitly perform triage, even if the work is not explicitly identified as such.

As the single point of entry for CSIRT correspondence, triage is on the critical path for all other CSIRT services.

This means it can also be a single point of failure.

Triage facilitates recognition and appropriate separation of

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

Triage can also be an effective tool for introducing new staff to the types of activity your CSIRT handles; the common terminology; how reports are handled, recorded and tracked; etc.

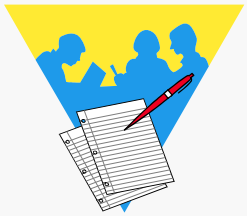
Balancing the workload produces a more equitable distribution of work across your staff.

CERT® Training and Education

Questions Addressed in Triage

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

- **What category and priority of report or request should 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.**



CERT® Training and Education

Categorization of Reports or Requests

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

- **type of service**
- **type of report or request**
- **type of activity**
- **priority or severity**
- **impact or scope**
- **escalation**

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

Priority or Severity Levels can be based on

- danger to human life
- amount of financial loss
- threat to CSIRT systems
- threat to Internet infrastructure
- type of activity

Impact or scope might involve

- complexity of attack
- number of systems at risk or affected
- success of attack
- active exploitation of a vulnerability

CERT® Training and Education

Elements that Support Triage

Triage is facilitated by the use of

- **reference numbers**
- **reporting forms**
- **a system for recording and tracking information**

These elements can help in facilitating the tracking, recording, and cross referencing of reports.

Forms can guide reporters (and CSIRT staff) to ensure that complete information is provided.

CERT® Training and Education

Reference Numbers

Why have reference numbers?

- triage automation
- internal tracking
- reference when communicating with others

Possible formats for reference numbers

- random numbers
- dated numbers
- combination

Consider formats that do not disclose sensitive data.

CERT® Training and Education

Reporting Forms

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

Use of a reporting form helps sites to

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

Use of a reporting form helps CSIRTs to

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

Examples of Reporting Forms

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

CERT® Training and Education

Recording & Tracking CSIRT Data -1

Decide what data your CSIRT needs to record and track to

- provide an effective response service
- correlating incident activity reports
- generate trend and statistical information

Ensure all data is recorded so that

- it can easily be searched
- anyone can pick up in the middle of an incident
- you can determine the current work load and distribution
- you can provide status updates to management
- you can prepare for possible legal action

CERT® Training and Education

Recording & Tracking CSIRT Data -2

Ensure processes are available for capturing and storing data from

- **telephone calls**
- **FAX messages**
- **other correspondence**

Provide support for handling encrypted data.

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

Record all action items associated with the handling of an incident, including assignments and deadlines.

The Incident Object Description and Exchange Format Working Group (IODEF WG) at TERENA has been working to “define 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/task-forces/tf-csirt/iodef/

This work has been presented in RFC 3067
http://www.ietf.org/rfc/rfc3067.txt

You may want to take a look at this standard as you create or enhance your incident reporting and tracking systems.

Best Practical Solutions LLC has developed an incident handling system, Request Tracker for Incident Response.
http://www.bestpractical.com/rtir/

CERAIS has developed an incident response database (CIRDB).
https://cirdb.cerias.purdue.edu/website/

CERT® Training and Education

Sample Incident Tracking System Fields

Contact information

Date and time
- of report
- of activity
- of discovery

Systems affected
- owner
- criticality and mission
- software and patch versions

Supplemental data gathered
- logs
- email
- artifacts

Description of problem
- overview
- in-depth technical information
- actions taken
- impact
- scope

Assigned staff

Action items

Staff contacted or interviewed

Cost/value
- damage
- recovery

CERT® Training and Education

Incident Handling Activities

Incident Handling Activities

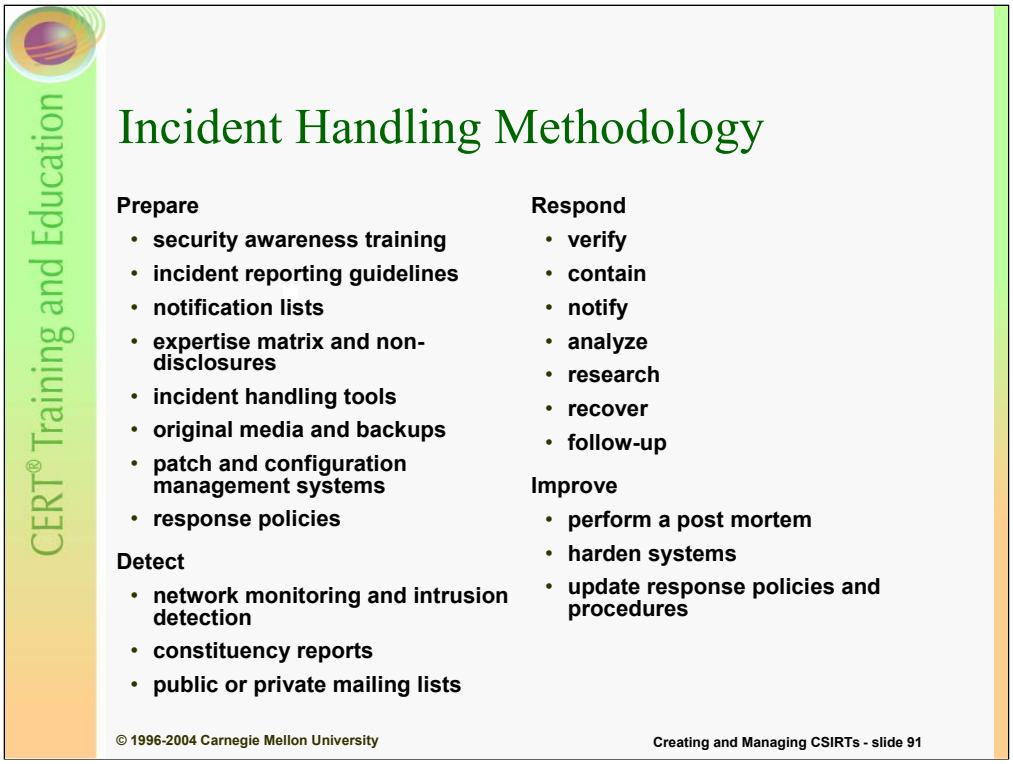
- **Critical Information**
- **Triage**
- **Coordinating Response**

CERT® Training and Education

Appropriate Response

Response options may include

- phone or email technical assistance
- on-site assistance
- analysis of logs, files, or other data
- investigative (legal) assistance, prosecution
- computer forensics
- development and dissemination of
  - patches, fixes, workarounds, or other solutions
  - advisories, alerts, technical documentation
- feedback to reporting site(s)
- none (forward to others to handle)



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

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 – who 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 not do. Work with IT to determine what systems need 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.

CERT® Training and Education

Sample Response Policies

Which incidents require further reporting to

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

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

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.**

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.

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

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.

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

What Are Major Events?

A major event is an incident or some other event or condition that affects your CSIRT response threshold.

This threshold will be determined by your CSIRT mission, policies, procedures, and constituency.

What constitutes a major event for one site may not be a major event at another site.

A major event is not necessarily one that involves a large number of sites.

CERT® Training and Education

What Is a Major Event for Your CSIRT Team?

- **one (1) machine at a site (e.g., your primary customer's public Web site)**
- **tens, hundreds, thousands of hosts or sites involved (or affected)**
- **mission critical or high-profile systems**
- **activity that exposes a site to potential damage (e.g., life-threatening, financial, legal)**
- **many sites affected by a vulnerability**
- **any system within your CSIRT**
- **any system within your parent organization**

Often a major event is the result of malicious activity or a concerted attack that is directed against sites

- within your constituency
- at your CSIRT

It can be the result of a software/hardware vulnerability or system misconfiguration.

It can be caused by lack of expertise in administration of the system(s) or network(s).

CERT® Training and Education

What Are Some Examples?

- emergence of sniffer incidents in 1994
- compromise of major software distribution site (mirrored many places)
- compromised Web pages at a high-profile site
- BIND vulnerability activity
- Melissa Macro Virus, March 1999
- Y2K incident reports
- VBS/LoveLetter VBScript Worm, May 2000
- Code Red Worm, Nimda Worm 2001
- SNMP vulnerabilities, 2002
- MS-SQL Server Worm, 2003

CERT® Training and Education

CSIRT Response -1

Follow normal procedures as defined by your policies and procedures.

- **prepare**
- **detect**
- **respond**
- **improve**

However, major events usually require a greater level of

- **prioritization of actions**
- **internal and external coordination of resources**
- **assistance to sites**
- **collaboration with external parties**

CERT® Training and Education

CSIRT Response -2

Changes in response procedures can include

- additional staff or coverage
- temporary changes in work assignments or hours
- quick turn around for analysis and announcements
- development of different types of documents or alerts
- escalation of activity to appropriate management, legal, or law enforcement organizations
- notification to collaborators, other CSIRTs, or public relations spokesperson
- higher than average interaction with the media
- collection of real-time statistics and reporting

CERT® Training and Education

What Has Worked Well?

Some recommendations

- Be proactive, create a plan.
- Create a special team with prioritized assignments.
- Prioritize what needs to happen and in what order.
- Create instructions and approved “talking points”.
- Increase coverage of hotline or help desk phone(s).
- Provide resources for callers and reporting sites.
- Provide initial resources for media.
- Keep your staff updated.
- Perform a Post-Mortem after the event.

CERT® Training and Education

Be Ready for Media Inquiries

- 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?

Anticipate media interest and plan accordingly.

Prepare standard response or FAQs to address queries.

CERT® Training and Education

Creating and Managing CSIRTs

- Introduction
- Creating an Effective CSIRT
- CSIRT Components
- Operational Management Issues
- Incident Handling Activities
- **Summary**

CERT® Training and Education

Summary

Managers 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 automation of incident handling tasks

Need easy way to collaborate and share information with others

Need easy and efficient way to sort through all incoming information

Required policies and procedures must be established and understood.

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/
- **Trusted Introducer Service for CSIRTs in Europe**
  http://www.ti.terena.nl/
- **Asia Pacific Computer Emergency Response Team (APCERT)**
  http://www.apcert.org/

- 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://interactive.sei.cmu.edu/news@sei/columns/security_matters/1999/mar/security_matters.htm
- **TF-CSIRT Task Force, Collaboration of CSIRTs in Europe**
  http://www.terena.nl/tech/task-forces/tf-csirt/

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

You may also want to think about

- attending a FIRST conference to meet others dealing with the same issues
- attending more CERT/CC CSIRT courses or a SANS conference to get more technical training

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

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/

CERT® Training and Education

CSIRT Requirements

Concept of Operations Document

Planning and Implementation

General CSIRT Policies and Procedures

Communications

Infrastructure

Staffing

CERT® Training and Education

Concept of Operations Document

Document the CSIRT vision

- defined constituency
- defined mission
- defined organizational home
- defined authority
- defined set of CSIRT services
- defined organizational model
- defined relationships: legal, human resources, IT, etc.
- defined CSIRT contact information
- defined CSIRT incident reporting guidelines

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

CERT 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

Mark Zajicek <mtz@cert.org>