What is a Computer Emergency Response Team (CERT)?

A Computer Emergency Response Team (CERT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident re-ports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client.

A CERT can be a formalized team or an ad-hoc team. A formalized team performs incident response work as its major job function. An ad-hoc team is called together during an ongoing computer security incident or to respond to an incident when the need arises.

What is a computer security incident?

Each organization will need to define what a computer security incident is for their site. Examples of general definitions for a computer security incident might be:

• 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

Examples of incidents could include activity such as

• attempts (either failed or successful) to gain unauthorized access to a system or its data

• unwanted disruption or denial of service

• unauthorized use of a system for the processing or storage of data

• changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

Computer security incident activity can be defined as network or host activity that potentially threatens the security of computer systems.

Why would an organization need a CERT?

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 way to respond.

The speed with which an organization can recognize, analyze, and respond to an incident will limit the damage and lower the cost of recovery. A CERT can be on site and able to conduct a rapid response to contain a computer security incident and recover from it. CERTs 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 CERTs and security organizations can facilitate the sharing of response strategies and early alerts to potential problems. Proactively, CERTs 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.

They can focus attention on security, and provide awareness training to the constituency. CERTs can also provide expertise to do preventive and predictive analysis to help mitigate future threats.

What types of CERT**s exist?**

CERTs come in all shapes and sizes and serve diverse constituencies. Some CERTs support an entire country, for example, the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC); others may provide assistance to a particular region, such as AusCERT does for the Asia-Pacific area; still others may provide support to a particular university or commercial organization. There are also corporate groups who provide CSIRT services to clients for a fee. Some general categories of CERTs include, but are not limited to, the following:

• **Internal** CERT**s** provide incident handling services to their parent organization. This could be a CSIRT for a bank, a manufacturing company, a university, or a federal agency.

• **National** CERT**s** provide incident handling services to a country. Examples include: the Japan CERT Coordination Center (JPCERT/CC) or the Singapore Computer Emergency Response Team (SingCERT).

• **Coordination Centers** coordinate and facilitate the handling of incidents across various CSIRTs. Examples include the CERT Coordination Center or the United States Computer Emergency Readiness Team (US-CERT).

• **Analysis Centers** focus on synthesizing data from various sources to determine trends and patterns in incident activity. This information can be used to help predict future activity or to provide early warning when the activity matches a set of previously determined characteristics.

• **Vendor Teams** handle reports of vulnerabilities in their software or hardware products. They may work within the organization to determine if their products are vulnerable and to develop remediation and mitigation strategies. A vendor team may also be the internal CERT for a vendor organization.

• **Incident Response Providers** offer incident handling services as a for-fee service to other organizations.

What other response team acronyms are there?

There is a wide variety of acronyms for incident response teams that exist around the world. Some of the more common acronyms are listed below:

CERT= Computer Emergency Response Team

CIRC= Computer Incident Response Capability

CIRT= Computer Incident Response Team

IRC= Incident Response Team

SERT= Security Emergency Response Team

SIRT= Security Incident Response Team

Where in an organizational structure is a CERT commonly found?

There is no standard hierarchical location where a CERT may be found in an organizational structure. Some CERT s are part of an existing Information Technology (IT) or Telecommunications group. Others may be part of a security group or work in conjunction with the group responsible for physical security. CERT s may also be located in the audit group, while others are in a separate entity. Many organizations are beginning to look at the development of a CERT as part of their business continuity and disaster recovery plans.

Wherever the CERT is located, it is vital that it has management support and receives authority to do the work required.

What does a CERT do? (What services does a Cert provide?) A Cert may perform both reactive and proactive functions to help protect and secure the critical assets of an organization. There is not one standard set of functions or services that a Cert provides. Each team chooses their services based on the needs of their constituency.

Whatever services a CERT chooses to provide, the goals of a CERT must be based on the business goals of its constituent or parent organizations. Protecting critical assets are key to the success of both an organization and its CERT. The CERT must enable and support the critical business processes and systems of its constituency.
A CERT is similar to a fire department. Just as a fire department "puts out a fire" that has been reported, a CERT helps organizations contain and recover from computer security breaches and threats. The process by which a CERT does this is called incident handling. But just as a fire department performs fire education and safety training as a proactive service, a CERT can also provide proactive services. These types of services may include security awareness training, intrusion detection, penetration testing, documentation, or even program development. These proactive services can help an organization not only prevent computer security incidents, but also decrease the response time involved when an incident occurs.

What is incident handling?
Incident handling includes three functions: incident reporting, incident analysis, and incident response.
The incident reporting function enables a CERT to serves as a central point of contact for reporting local problems. This allows all incident reports and activity to be collected in one location where information can be reviewed and correlated across the parent organization or constituency. This information can then be used to determine trends and patterns of intruder activity and recommend corresponding preventative strategies for the whole constituency. This is one part of the incident analysis function. The other part of incident analysis involves taking an in-depth look at an incident report or incident activity to determine the scope, priority, and threat of the incident, along with researching possible response and mitigation strategies.
Incident response functions can take many forms. A CERT may send out recommendations for recovery, containment, and prevention to constituents or systems and network administrators at sites who then perform the response steps themselves. A CERT may also perform these steps themselves on the affected systems. The response may also involve sharing information and lessons learned with other response teams and other appropriate organizations and sites.
These incident handling functions are the reactive services that a CERT may provide.

How big should a CERT be?
Determining the size of a CERT can be a challenge, and unfortunately there is little empirical data that can be used to answer this question. Different CERTs have different staffing levels based on their resources, needs and workload. A model that works for one organization may not work for another.
The size of CERT staff should be based on the resources available and the services that are necessary to provide. Experience has shown that no team wants a single point of failure, so just having one person devoted to incident response may not be enough.

Who works in a CERT?

Our experience has shown that the best CSIRT staff members have a variety of technical skills and personality traits (including communication skills and people skills). CSIRT staff are dedicated, innovative, detail-oriented, flexible, and analytical. They are problem solvers, good communicators, and able to handle stressful situations. One of the most important traits a team member must have is integrity.

CERT staff roles may include
- manager or team leader
- assistant managers, supervisors, or group leaders
- hotline, help desk, or triage staff
- incident handlers
- vulnerability handlers
- artifact analysis staff
- platform specialists
- trainers
- technology watchers

Other roles may include
- support staff
- technical writers
- network or system administrators, CERT infrastructure staff
- programmers or developers (to build CERT tools)
- web developers and maintainers
- media relations staff
- legal or paralegal staff or liaison
- law enforcement staff or liaison
- auditors or quality assurance staff
- marketing staff

Where can an organization find more information on CERT policies and procedures?

Issues related to CSIRT policies and procedures are included in the *Handbook for Computer Security Incident Response Teams (CSIRTs)* (see Section 2.5.).

Another useful online resource for information security policies, although not specifically related to CSIRTS, is the SANS Security Policy Project page, which includes sample policies and policy templates as well as links to other websites containing information security policies.

Other collections of various types of computer policies include the following:
- EDUCAUSE/Cornell Institute for Computer Policy and Law
- *Information Security Policies Made Easy* (10th Edition), Charles Cresson Wood, Houston, Texas: Information Shield, 2005.

What is FIRST?

FIRST is the international forum of incident response and security teams. Established in1990, FIRST is a coalition that brings together a variety of security teams and computer security incident response teams from government, commercial, and academic organizations. Attending the yearly FIRST conferences can be a way for a new team to learn more about techniques and strategies for providing a response capability as well as to get in contact with established teams.
You can learn more about FIRST on their web page. If you would like to become a member, please refer to the FIRST membership page.