CSIRT FREQUENTLY ASKED QUESTIONS (FAQ)

What is a Computer Security Incident Response Team (CSIRT)?

A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports 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 CSIRT 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 CSIRT?

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 CSIRT can be on site and able to conduct a rapid response to contain a computer security incident and recover from it. 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 the sharing of response strategies and early alerts to potential problems. Proactively, 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.

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

What types of CSIRTs exist?

CSIRTs come in all shapes and sizes and serve diverse constituencies. Some CSIRTs 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 CSIRTs include, but are not limited to, the following:

- **Internal CSIRTs** 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 CSIRTs** 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 CSIRT 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:

Acronym	**Definition**
CSIRT	Computer Security Incident Response Team
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
IRC	Incident Response Center or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

Can "CERT" be used in a CSIRT name?
"CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office. Organizations who wish to use "CERT" in their team name must contact us to request permission. For additional copyright information about the CERT Division, please see our legal information. For additional information about the CERT Coordination Center, see the CERT FAQ.

Where in an organizational structure is a CSIRT commonly found?
There is no standard hierarchical location where a CSIRT may be found in an organizational structure. Some CSIRTs 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. CSIRTs 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 CSIRT as part of their business continuity and disaster recovery plans.

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

What does a CSIRT do? (What services does a CSIRT provide?)
A CSIRT 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 CSIRT provides. Each team chooses their services based on the needs of their constituency. For a discussion of the wide range of services that a CSIRT can choose to provide, please see Section 2.3 of the *Handbook for CSIRTs*.

Whatever services a CSIRT chooses to provide, the goals of a CSIRT 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 CSIRT. The CSIRT must enable and support the critical business processes and systems of its constituency.

A CSIRT is similar to a fire department. Just as a fire department "puts out a fire" that has been reported, a CSIRT helps organizations contain and recover from computer security breaches and threats. The process by which a CSIRT does this is called incident handling. But just as a fire department performs fire education and safety training as a proactive service, a CSIRT 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 CSIRT 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 CSIRT 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 CSIRT 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 CSIRT may provide.

Who provides the funding for a CSIRT?

CSIRTs can receive funding from their parent organization, either directly or as part of an IT department (e.g., a CSIRT formed from existing staff members of a commercial organization, a university, a government/military organization). The CSIRT could also be funded via some other mechanism—a membership subscription service (members subscribe to selected services that the CSIRT provides and pay a fee for those services), through government services, via a network service provider, perhaps through project funding, etc.

How much does it cost to create a CSIRT?

The cost to create a CSIRT will depend on the number of resources and services to be provided, the administrative costs for the area or organization, and the structure of the CSIRT.

While information about the costs of creating a CSIRT is not widely available, there are some resources that may help determine the cost of computer security incidents and response strategies. This information may be used to help determine the resources needed to prevent or recover from an incident. This information may also be used in a cost/benefit analysis to compare the cost of an incident to the cost of preventing the incident or decreasing the recovery time by implementing a CSIRT.

Developing an Effective Incident Cost Analysis Mechanism, by David A. Dittrich; SecurityFocus, June 12, 2002 http://www.securityfocus.com/infocus/1592

Incident Cost Analysis and Modeling Project
https://www.cic.net/docs/default-source/reports/icampreport2.pdf?sfvrsn=0

Computer Crime and Security Survey from Computer Security Institute (CSI) in partnership with the FBI
http://reports.informationweek.com/abstract/21/7377/research-2010-2011-csi-survey.html

Australian Computer Crime and Security Surveys 2002-2006
https://www.auscert.org.au/crimesurvey

How big should a CSIRT be?

Determining the size of a CSIRT can be a challenge, and unfortunately there is little empirical data that can be used to answer this question. Different CSIRTs 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 CSIRT 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 CSIRT?

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.

CSIRT 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, CSIRT infrastructure staff
- programmers or developers (to build CSIRT 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

What type of CSIRT training is required?

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 to learn about your

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

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

- SEI courses in information security and CSIRTs
- SANS Training
- Global Information Assurance Certification (GIAC) Program

Where can an organization find more information on CSIRT 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.

How does an organization start a CSIRT?

There are several components to building an effective CSIRT. The actual process for building a team will depend on the timeframes, available staff and budget resources, expertise, and the unique circumstances of each organization. The following is a high-level overview of some of these components; some are sequential and some can be handled in parallel, depending on the resources and level of support obtained from the organization:

- Obtain management support and buy-in. Without management support it will be very difficult for the CSIRT to obtain the funding, staffing, and resources to be a success.
- Meet with key stakeholders to define the overall strategic goals of the CSIRT and to understand the needs of the constituency and services the CSIRT will offer.
- Design the CSIRT vision based on discussions about the:
    - constituency to be served by the CSIRT
    - mission, goals and objectives of the CSIRT
    - services provided by the CSIRT
    - organizational model that is most appropriate for the CSIRT and the relationship it has with the parent organization or customer base
    - funding to support the CSIRT start-up costs and costs to sustain its operations
    - resources needed by the CSIRT
- Communicate the CSIRT vision and operational plan to its management, constituency, and others who need to know and understand the operations.
- Obtain feedback and refine the vision and plan.
- Once this "buy-in" and support is obtained, implement the CSIRT. The implementation will include
    - hiring and training the CSIRT staff

- purchasing equipment and building the CSIRT infrastructure to support the team and the needs of the constituency
- developing CSIRT policies and procedures to support the day-to-day operations and long-term goals and objectives
- developing incident reporting guidelines for the constituency, and ensuring they have access to and understand the incident reporting guidelines
- announcing the operational CSIRT to the community at large
- identifying a mechanism to evaluate the effectiveness of the CSIRT (e.g., feedback from the constituency) and improving CSIRT processes as needed

The CERT Division offers a one-day course that focuses on providing guidance and additional insight that can help organizations plan and implement their response team. In addition, two documents that provide an overview of issues to be considered when starting a CSIRT are

- Forming an Incident Response Team examines the role a response team may play in the community and the issues that should be addressed both during the formation and after commencement of operations. This paper was written by a member of the Australian Computer Emergency Response Team.
- *Handbook for Computer Security Incident Response Teams (CSIRTs)* provides guidance about the generic issues to consider when forming and operating a CSIRT. In particular, it helps an organization to define and document the nature and scope of a computer security incident response service, which is the core service of a CSIRT, as well as examine how to create the CSIRT policies and procedures. The second edition of this handbook was updated and published in 2003.

Other resources that provide information about interacting with other CSIRTs, as well as guidelines for developing computer security policies and procedures, include the following:

- Expectations for Computer Security Incident Response (RFC 2350)
- Site Security Handbook (RFC 2196)
- Avoiding the Trial-by-Fire Approach to Security Incidents

The CERT Division also offers other training courses for those who will manage a CSIRT as well as for technical staff who want more training in analyzing and responding to computer security incidents.

Where can I find a list of CSIRTs?
You can find links to other CSIRT teams on the FIRST site.

What is FIRST?
FIRST is the international forum of incident response and security teams. Established in

1990, FIRST is a coalition that brings together a variety of security teams and computer security incident response teams from government, commercial, and academic organizations. Attending the yearly FIRST conferences can be a way for a new 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.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0004385