CERT | Software Engineering Institute
Carnegie Mellon University

CREATE A CSIRT

Background

Keeping organizational information assets secure in today's interconnected computing environment is a true challenge that becomes more difficult with each new "e" product and each new intruder tool. Most organizations realize that there is no one solution or panacea for securing systems and data; instead a multi-layered security strategy is required. One of the layers that many organizations are including in their strategy today is the creation of a Computer Security Incident Response Team, generally called a CSIRT.

Motivators driving the establishment of CSIRTs include

- a general increase in the number of computer security incidents being reported
- a general increase in the number and type of organizations being affected by computer security incidents
- a more focused awareness by organizations on the need for security policies and practices as part of their overall risk-management strategies
- new laws and regulations that impact how organizations are required to protect information assets
- the realization that systems and network administrators alone cannot protect organizational systems and assets

What Are the Questions?

As organizations begin to build their incident response capability, they are looking to determine the best strategy for putting such a structure in place. They not only want to know what has worked well for others, but also want some guidance on the process and requirements they must follow to establish an effective incident response capability.

CSIRTs and their parent organizations have numerous questions they want answered to help them design their response capability. They are also interested in knowing what other teams in similar industry sectors are doing. Typical questions being asked include but are not limited to the following:

- What are the basic requirements for establishing a CSIRT?
- What type of CSIRT will be needed?
- What type of services should be offered?
- How big should the CSIRT be?

- Where should the CSIRT be located in the organization?
- How much will it cost to implement and support a team?
- What are the initial steps to follow to create a CSIRT?

There is not a standard set of answers to these questions. CSIRTs are as unique as the organizations they serve, and as a result, no two teams are likely to operate in the exact same manner. It is important for the organization to decide why it is building a CSIRT and what it wants that CSIRT to achieve. Once this is determined, then the unique set of answers to these questions can be formulated.

This document is the first in a series that will discuss the issues and decisions to be addressed when planning and implementing a CSIRT. This first document focuses on an overview of the basic high-level steps to be taken by organizations as they design and build a CSIRT. The document is written as a general guideline for any organization that is thinking about undertaking such an endeavor or for any individuals who are members of a project team that is working to establish a CSIRT.

What Are Some Best Practices for Creating a CSIRT?

Although CSIRTs will differ in how they operate depending on the available staff, expertise, budget resources, and unique circumstances of each organization, there are some basic practices that apply to all CSIRTs. We will discuss some of those practices as they relate to creating a CSIRT. (For more information on what a CSIRT is, see the CSIRT FAQ.) Although these actions are presented as steps, the process is not sequential; many steps can occur in parallel.

The steps are as follows:

- Step 1: Obtain management support and buy-in
- Step 2: Determine the CSIRT strategic plan
- Step 3: Gather relevant information
- Step 4: Design the CSIRT vision
- Step 5: Communicate the CSIRT vision and operational plan
- Step 6: Begin CSIRT implementation
- Step 7: Announce the operational CSIRT
- Step 8: Evaluate CSIRT effectiveness

Step 1: Obtain Management Support and Buy-In

Our experience shows that without management approval and support, creating an effective incident response capability can be extremely difficult and problematic. This support must be shown in numerous ways, including the provision of resources, funding, and time, to the person or group of people who will act as the project team for implementing the CSIRT. This also includes executive and business or department managers and their staffs committing time to participate in this planning process; their input is essential during the design effort.

It is important to elicit management's expectations and perceptions of the CSIRT's function and responsibilities. Without this information, a team may be built whose services and authority are not understood or appropriately used by the rest of the organization.

Along with obtaining management support for the planning and implementation process, it is equally important to get management commitment to sustain CSIRT operations and authority for the long term. Once the team is established, how is it maintained and expanded with budget, personnel, and equipment resources? Will the role and authority of the CSIRT continue to be backed by management across the various constituencies or parent organization? Without this continued support, the CSIRT's long-term success may be in jeopardy.

Step 2: Determine the CSIRT Development Strategic Plan

Think about how to manage the development of the CSIRT. What administrative issues must be dealt with, and what project management issues must be addressed?

- Are there specific time frames to be met? Are they realistic, and if not, can they be changed?
- Is there a project group? Where do the group members come from? You want to ensure that all stakeholders are represented. Some may not be on the team for the whole project, but brought in to provide subject matter expertise and input as needed. You also want to incorporate best practices in project management, organizational behavior theory, and communications theory into your plan. If anyone has a background in these areas, consider having them participate on the team.
- How do you let the organization know about the development of the CSIRT? A memo sent from the CIO, CEO, or other high-level manager announcing the project and asking each key stakeholder and area to provide assistance in any way possible is a good way to start. Letting the organization know about the plan for a CSIRT in the early stages of development can help staff feel they are part of the design process.
- If you have a project team, how do you record and communicate the information you are collecting, especially if the team is geographically dispersed?

Step 3: Gather Relevant Information

Gather information to determine the incident response and service needs that the organization has. Take a look at the types of incident activity currently being reported within your constituency. This helps determine not only what type of services to offer, but also the types of skills and expertise the CSIRT staff will need. For example, if your organization has been the victim of computer virus or worm activity, you will need staff with virus experience to handle the response. You will also need virus scanning, elimination, and recovery procedures, along with the appropriate anti-virus tools. You may want people with good training and documentation skills to help develop user awareness programs as a proactive step in dealing with virus activity.

Identify what information you need to know to plan and implement the CSIRT. Determine who has that information and how best to elicit that information, either through general discussions or interviews or by making them part of the project.

Meet with key stakeholders to discuss not only their incident response needs, but to achieve an initial consensus on the expectations, strategic direction, definitions, and responsibilities of the CSIRT. Your definition of what a CSIRT is and does may be very different from your manager's definition or the definition of another part of your organization. Use these discussions with the stakeholders to outline and identify how each group will need to interact with the CSIRT. The stakeholders could include but are not limited 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 do the IT staff and the CSIRT interact? What actions are taken by IT staff and what actions are taken by CSIRT members during response operations? Will the CSIRT have easy access to network and systems logs for analysis purposes? Will the CSIRT be able to make recommendations to improve the security of the organizational infrastructure?
- **Representatives from the legal department**. When and how is the legal department involved in incident response efforts? Legal staff may also be needed to review non-disclosure agreements, develop appropriate wording for contacting other sites and organizations, and determine site liability for computer security incidents.
- **Representatives from human resources**. They can help develop job descriptions to hire CSIRT staff, and develop 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 vulnerability assessments, along with encouraging computer security best practices across the constituency or organization.
- **General representatives from the constituency**. They can provide insight into their needs and requirements.

Stakeholders should also include anyone who will be involved in the incident-handling or notification process. Think about who will need to be notified during different types of incidents. Are there people in other parts of the organization or constituency who can provide information or input to the CSIRT or with whom the CSIRT will need to share or obtain information? These may include other parts of the IT or security departments, including any groups doing vulnerability assessments, intrusion detection, or network monitoring. Knowing what the CSIRT will need to do can help you identify the right people to be involved in developing the procedures.

Find out if anyone else is currently performing any of the services that the CSIRT may be looking to provide. Determine if those services should stay with the current group or move to the CSIRT over some agreed-to period of time. Addressing these types of issues in the planning stages can help identify what responsibilities will need to be delineated and what information will need to be gathered.

There may also be some resources available for review that will help in your information gathering. These may include

- 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-management plans
- any parental or institutional regulations
- any existing security policies and procedures

Reviewing these documents serves a dual purpose: first, to 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, 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. Such lists may be adapted for CSIRT work and processes.

In addition, 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. Take a look at other CSIRTs' websites, and check their missions, charters, funding scheme, and service listing. This may give you ideas for organizing your team. Review any books or other publications about incident handling or CSIRTs. An initial list of resources can be found on the CERT CSIRT Development page.

Attend courses or conferences that include sessions for developing incident response strategies or creating CSIRTs. These venues can provide you with opportunities to exchange ideas and interact with others in the incident response field. A good place to start may be to attend the annual FIRST conference.

Step 4: Design Your CSIRT Vision

As the information gathered brings to the forefront the incident response needs of the constituency and as you build your understanding of management expectations, you can begin to identify the key components of the CSIRT. This allows you to define the vision for the CSIRT and its goals and functions.

You need both management and constituent buy-in and support of these goals and functions for the CSIRT to be successful.

It is important to achieve clear agreement on the definition and expectations for the CSIRT being formed. What the CSIRT staff thinks the team will do and what the managers and general constituency think the CSIRT will do may be completely different. A number of people have the perception that a CSIRT is a "cyber cop" for an organization or constituency. While this may be true for a small number of teams, it is not generally the main focus of a CSIRT. The main focus is to prevent and respond to incidents. The vision for the CSIRT must include a clear explanation of where these CSIRT functions fit into the current organizational structure and how the CSIRT interacts with its constituency. The vision explains what benefits the CSIRT provides, what processes it enacts, who it coordinates with, and how it performs its response activities.

In creating your vision, you should

- Identify your constituency. Who does the CSIRT support and serve?
- Define your CSIRT mission, goals, and objectives. What does the CSIRT do for the identified constituency?
- Select the CSIRT services to provide to the constituency (or others). How does the CSIRT support its mission?
- Determine the organizational model. How is the CSIRT structured and organized?
- Identify required resources. What staff, equipment, and infrastructure are needed to operate the CSIRT?
- Determine your CSIRT funding. How is the CSIRT funded for its initial startup and its long-term maintenance and growth?

Step 5: Communicate the CSIRT Vision

Communicate the CSIRT vision and operational plan to management, your constituency, and others who need to know and understand its operations. As appropriate, make adjustments to the plan based on their feedback.

Communicating your vision in advance can help identify process or organizational problems before implementation. It is a way to let people know what is coming and allow them to provide input into CSIRT development. This is a way to begin marketing the CSIRT to the constituency and gaining the needed buy-in from all organizational levels.

You may receive information that was missed or not available during the information-gathering stage. Use this information and input to make any final adjustments to the CSIRT organizational structure and processes.

Step 6: Begin CSIRT Implementation

Once management and constituency buy-in is obtained for the vision, begin the implementation:

- Hire and train initial CSIRT staff.
- Buy equipment and build any necessary network infrastructure to support the team.
- Develop the initial set of CSIRT policies and procedures to support your services.
- Define the specifications for and build your incident-tracking system.
- Develop incident-reporting guidelines and forms for your constituency.

A main resource you will need for your constituency is your incident-reporting guidelines. These guidelines define how your constituency interacts with your CSIRT, what constitutes an incident, what types of incidents to report, who should report an incident, why an incident should be reported, the process for reporting an incident, and the process for responding to an incident. They should be clear and understandable by the constituency being served.

The process for reporting an incident includes a detailed description of the mechanisms for submitting reports: phone, email, web form, or some other mechanism. It should also include details about what type of information should be included in the report.

The process for responding to an incident details how the CSIRT prioritizes and handles received reports. This includes how the person reporting an incident is notified of its resolution, any response time frames that must be followed, and any other notification that occurs.

Step 7: Announce the CSIRT

When the CSIRT is operational, announce it broadly to the constituency or parent organization. It is best if this announcement comes from sponsoring management. Include the contact information and hours of operation for the CSIRT in the announcement. This is an excellent time to make available the CSIRT incident-reporting guidelines. You may also want to develop information to publicize the CSIRT, such as a simple flyer or brochure outlining the CSIRT mission and services, which can be distributed with the announcement. Some teams have held an open house or special celebration to announce the operational CSIRT.

Step 8: Evaluate the Effectiveness of the CSIRT

Once the CSIRT has been in operation for a while, management will want to determine the effectiveness of the team and use evaluation results to improve CSIRT processes and ensure that the team is meeting the needs of the constituency. The CSIRT, in conjunction with management and the constituency, will need to develop a mechanism to perform such an evaluation.

Information on effectiveness can be gathered through a variety of feedback mechanisms, including

- benchmarking against other CSIRTs
- general discussions with constituency representatives

- evaluation surveys distributed to constituency members on a periodic basis
- creation of a set of criteria or quality parameters that is then used by an audit or third party group to evaluate the team

It may be helpful to review 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. Information collected for comparison may include

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

See Section 2.2.4 of the *Handbook for Computer Security Incident Response Teams* for more information on evaluating the quality of CSIRT services.

Remember that Patience Can Be a Key

The length of time it will take to design, plan, and implement a team will vary with each organizational situation. We have seen CSIRTs become operational across a wide range of times, from two months to two years. It is important to realize that it can take about 12-18 months to work out the processes and procedures, especially for a large, distributed enterprise. After the team is operational, it can take another 12-18 months to obtain a good level of trust and comfort with your constituency. Many teams show a large growth in the number of incidents reported over their first year of operation. The longer you are in operation, the more your constituency will understand the work you are doing and the more likely they will report incidents to you.

Resources and More Information on Creating a CSIRT

The components discussed above are more fully discussed in the following:

- Creating a CSIRT Workshop (CERT/CC one-day workshop)
- Handbook for Computer Security Incident Response Team

These resources may provide additional insight:

- Forming an Incident Response Team
  A paper examining 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 former member of the Australian Computer Emergency Response Team.

- Expectations for Computer Security Incident Response (RFC 2350)
  This is a best practices document that recommends general requirements and behaviors that a CSIRT should follow when establishing or operating a team. It focuses on methods for letting the CSIRT constituency know about the team's services and processes.
- Avoiding the Trial-by-Fire Approach to Security Incidents
  This article discusses the importance of having an organized and defined process for detecting and responding to computer security incidents.

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-0004387