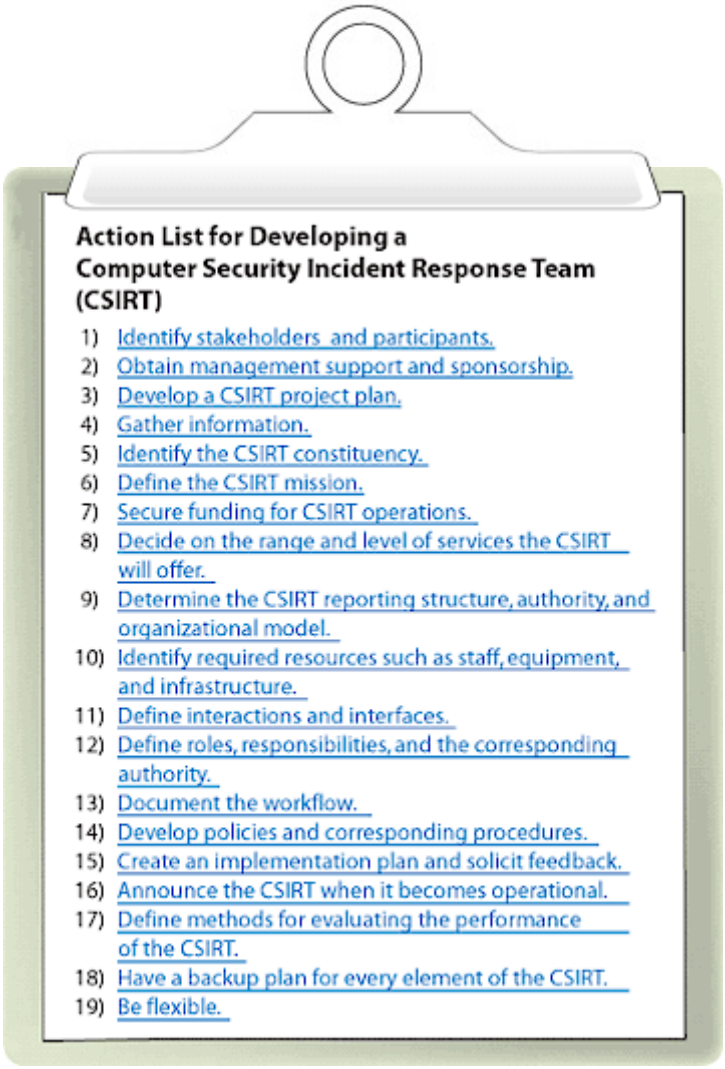
Action List for Developing a Computer Security Incident Response Team (CSIRT)

This document provides a high-level overview of actions to take and topics to address when planning and implementing a Computer Security Incident Response Team (CSIRT). It also identifies some common problems teams may encounter in their implementation. The list draws on material presented in depth through CERT training courses and publications, and incorporates lessons learned by staff during their experiences planning and implementing CSIRTs. Use this list as a starting point to plan a CSIRT. More detailed information can be found in the list of resources at the end of this article.



1) Identify stakeholders[1] and participants.

a. Determine who needs to be involved at each level of the CSIRT planning, implementation, and operation.
b. Determine who is served or supported by the CSIRT.
c. Identify people with whom you will coordinate or share information, both inside and outside the organization. (You may want to talk with them as you gather information. Consider asking them to participate in the development project or to

help review CSIRT design and implementation plans.)
d. Identify people performing security or incident response functions and talk to them.
e. Identify which internal and external organizations might interface with or participate in the CSIRT.

Common problems: a full range of stakeholders and participants are not identified and included in the planning and development phase; failure to identify and understand where computer security incident response activities are performed and how this will change with any new plans for a CSIRT.

2) Obtain management support and sponsorship.

a. Find an executive manager to sponsor and champion the CSIRT's establishment. This person can be a good liaison to other executive and business managers in the constituency[2] or parent organization.
b. Present a business case to management outlining the benefits the CSIRT will bring to the organization or constituency.
c. Obtain management support for the time and resources the team will spend researching and gathering information during the planning process.
d. If establishing a CSIRT within an organization, explain the ideas, concepts, and benefits to other business function managers.
   If establishing a national team, explain the concepts and benefits to key organizations and potential strategic partners that will be supported by the CSIRT.
e. Request management to announce the formation of the CSIRT project and ask people to provide information as needed during the planning and implementation phases.

Common problems: relevant stakeholders, participants, business managers, and strategic partners are not aware that a CSIRT is being planned.

3) Develop a CSIRT project plan.

a. Form a project team to help plan and establish the CSIRT.
b. Appoint a project leader. This person can inform management about the progress made in planning.
c. Apply project management concepts to the task of setting up a CSIRT.

Common problems: the project team does not involve a diverse set of stakeholders; a reasonable timeframe is not established for the project's completion – often timeframes are too short or unrealistic for a CSIRT to become fully operational; a project leader is not established and the project languishes without direction or completion.

4) Gather information.

a. Hold conversations with a variety of stakeholders to
   - determine the needs and requirements of the constituency and any parent or host organization.
   - collect information about types of incidents already occurring to better understand the expertise and services the CSIRT will need to provide.
   - understand any incident management or response that is already occurring.
   - understand legal, political, business, or cultural issues that will define the environment in which the CSIRT will operate.

    - understand data ownership and intellectual property (IP) issues and authority, related to any type of publications, products, or information collected or developed by the CSIRT.
b. Define political and compliance[3] issues, including any public, private, academic, government, or military rules, regulations, or policies that must be followed or addressed as the CSIRT is established.
c. Understand the previous history.
    - Find out if anyone attempted to create a CSIRT in the organization before. If so, find out what happened and check for any information you can use.
    - Identify any organizational expectations of the CSIRT, based on this previous activity, that the team will need to correct.
    - Determine if the desired domain name is available (i.e., if the CSIRT will have its own domain name). If the name is available, obtain it as soon as possible.

Common problems: the CSIRT does not involve or gather input from all stakeholders; there are disagreements over who owns the data and intellectual property which can cause delays in providing CSIRT information to the constituency.

5) Identify the CSIRT constituency.

a. Determine the initial group of individuals or organizations to which the CSIRT will provide service and support.
b. Identify what types of services the CSIRT will provide to different segments of the constituency. For example, services provided to the general public may be different than services provided to government organizations or critical infrastructures. Understanding the constituency will also help define what groups to target for marketing CSIRT services.
c. Identify and establish strategic partners, if applicable. Strategic partners can
    - help guide the priorities and direction of the CSIRT, and help define and mature the CSIRT's capabilities and services.
    - engage in information sharing and research.
    - participate in customized interactions with the CSIRT.
    - help increase the visibility and influence of the team.
    - help promote the adoption and use of security best practices throughout the enterprise or constituency.
d. Identify how the constituency members obtain services from the CSIRT.
e. Identify constituents that the CSIRT may not initially support, but may support in the long term, after the CSIRT has been operational and is ready to expand its services.

Common problems: not all constituents are addressed or defined, so they have no formal interface with the CSIRT; the CSIRT does not properly create an understanding of the benefits its services can provide for the defined constituency; it is not clear how the constituency should contact the CSIRT and obtain assistance; the CSIRT tries to support too many diverse constituencies during its startup.

6) Define the CSIRT mission.

a. Determine the mission of the CSIRT. This process is long term and general in nature. The mission should not change much over time, so it should be written broadly enough to accommodate any change in services or functions while still succinctly defining the purpose and function of the CSIRT. The mission statement should provide value to both the constituency and the parent or host

organization.
b. Determine the primary goals and objectives of the CSIRT. These will be more practical and may be changed as the CSIRT expands its scope or services.
c. Obtain agreement on the mission from all relevant stakeholders (e.g., management, constituency, collaborators, and staff); ensure everyone understands the mission.

Common problems: staff don't understand the mission and "mission creep"[4] occurs (the CSIRT loses focus on its defined purpose and becomes less effective); outside parties (such as politicians) may have a perspective on the mission that doesn't match the CSIRT mission and try to pull the team into activities it is not prepared to handle.

7) Secure funding for CSIRT operations.

a. Obtain funding for start-up, short-term and long-term operations. This will include
    - initial staffing, short-term and long-term professional development, and training.
    - equipment, tools, and network infrastructure for detecting, analyzing, tracking, and responding to computer security incidents.
    - facilities for protecting and securing CSIRT data, systems, and staff.
b. Decide what funding model you will use to support the CSIRT; this could include fee-for-service, membership subscriptions, government sponsorship, or a parent organization budget line.

Common problems: CSIRTs can lose effectiveness by not funding efforts to help staff keep up with emerging technologies or by not enabling staff to attend conferences and training to improve their skills, knowledge, and abilities; this can make the team less able to handle new threats, attacks, and risks that affect their constituency.

8) Decide on the range and level of services the CSIRT will offer.

a. Start small and grow. Be realistic about the type and number of services the new CSIRT can provide given existing expertise and resources.
b. Determine the services the CSIRT will provide and identify to which part of the constituency they will be offered.
c. Define the process for delivery of services (e.g., hours of operation, contact methods, methods for information dissemination, and related processes).
d. Decide how the CSIRT will market its service.

Common problems: people want the CSIRT to perform services before it is ready; trying to offer too many services at once; trying to play too many roles; creating services that are not needed or that another organization is offering; not marketing needed services.

9) Determine the CSIRT reporting structure, authority, and organizational model.

a. Determine where the CSIRT will fit into the organizational structure. For instance, a national-level CSIRT may function within the government, as a separate national entity, or as part of another organization. If placed within another organization, how is it perceived by the constituency and how will those perceptions affect its operation?
b. Create an organization chart and keep it current.

c. Determine if the CSIRT must report “up” the hierarchy to any other organization or parent entity.
d. Prepare to educate people about the work the CSIRT will be able to do. Team members may need to diplomatically refuse some work requests and should prepare appropriate responses.

Common problems: non-CSIRT assignments are imposed by outside stakeholders that take staff away from their primary CSIRT functions and inhibit effective performance of normal services.

10) Identify required resources such as staff, equipment, and infrastructure.

a. Determine how the CSIRT infrastructure will be protected, secured, and monitored, especially the physical premises and data repositories.
b. Define processes for collecting, recording, tracking, and archiving information.
c. Create job descriptions that list the required knowledge, skills, and abilities (KSAs) for each CSIRT position.
d. Create a mentoring and training plan for staff, and ensure they are cross-trained on unique expertise or services.
e. Determine requirements for appropriate background checks, certifications, or security clearances.

Common problems: staff is not cross-trained, resulting in ‘single points of failure’ if someone performing a function requiring a unique skill leaves; staff are not given opportunity and a path for professional or career development, resulting in burnout and high levels of job turnover.

11) Define interactions and interfaces.

a. Identify interactions and interfaces with key parts of the constituency, stakeholders, and with any internal or external partners, collaborators, or contractors.
b. Determine what other entities the CSIRT will coordinate with.
c. Identify how information flows between these entities.
d. Define and establish interfaces and methods of collaboration and communication with others as appropriate, including law enforcement, vendors, critical infrastructure components, internet service providers (ISPs), other security groups, and other CSIRTs.
e. Ensure there are good methods for internal communication among the CSIRT staff.
f. For all these interfaces, understand
    - who owns the data that is shared.
    - who has authority and responsibility for data.
    - how the data is shared and with whom it is shared.
    - how the data is protected, controlled, and securely stored.
g. Define methods to disseminate information to the constituency and relevant stakeholders.
h. Develop and explain standard document types for disseminating information to the constituency.

Common problems: data is not shared in a controlled and secure manner, resulting in confidences being broken; CSIRT staff is not informed about CSIRT activities, reducing effectiveness in normal work roles; defined interfaces are not established, causing a process breakdown when escalation or data sharing and coordination is required.

12) Define roles, responsibilities, and the corresponding authority.

a. Develop roles and responsibilities for all CSIRT functions.
b. Define and develop the interfaces between CSIRT functions and other external functions and collaborations.
c. Identify areas where authority may be ambiguous or overlapping, and define functions and roles between groups.

Common problems: people don't know where their role ends and someone else's begins; more than one group is given the same responsibility; no one is given a specific responsibility and the task is never completed.

13) Document the workflow.

a. Create a diagram (swimlane chart, flow chart, etc.) to document the CSIRT processes and corresponding interactions, including who performs the work and where in the process the interfaces and handoffs occur.
b. Build quality assurance measures and components into the CSIRT processes and corresponding workflows.

Common problems: staff is uncertain how to follow certain processes or perform various coordination and collaboration activities.

14) Develop policies and corresponding procedures.

a. Establish definitions for terminology (e.g., "computer security event and incident") along with other terms unique to the organization.
b. Determine corresponding incident categories, priorities, and escalation criteria.
c. Identify initial policies and procedures that need to be formalized before operation, and those that can be created after the CSIRT is operational.
d. Develop incident reporting guidelines for the constituency and ways to publicize them.
e. Define and document criteria for providing CSIRT services to ensure consistent, reliable, and repeatable processes are followed by staff.

Common problems: common definitions are not shared between the CSIRT and constituency, resulting in confusion and misunderstanding; inability to summarize data on incident trends because there is no clear definition of terms; lack of formalized policies can delay response time because processes must be defined each time an incident occurs.

15) Create an implementation plan and solicit feedback.

a. Obtain input about the implementation plan from stakeholders and constituents (or other CSIRT experts), ask for their comments, and ensure the plan matches the mission.
b. Update and improve the plan based on feedback.
c. Obtain management and constituent support for the implementation.

Common problems: the constituency is not informed about the CSIRT implementation and does not provide support, which may result in incidents not being reported to the CSIRT or CSIRT advice and recommendations not being followed; the implementation plan is not sent for review, resulting in a plan that is not supported or implemented.

16) Announce the CSIRT when it becomes operational.

a. Ask management to make a formal announcement.
b. Provide marketing materials and incident reporting guidelines explaining how the constituency should interact with the CSIRT.
c. Incorporate training about CSIRT services and interactions into staff orientation programs.
d. Find ways to disseminate information about CSIRT services such as organizational intranets, web sites, brochures, seminars, and training classes.

Common problems: the CSIRT is not formally announced, and no one understands how or when to interface with the team.

17) Define methods for evaluating the performance of the CSIRT.

a. Define baselines for incident reporting and handling within the organization before the CSIRT is implemented. Use the baselines to compare performance once the CSIRT is operational.
b. Define measurement criteria and quality assurance parameters so that the CSIRT can be measured in a consistent way.
c. Define methods for obtaining constituency feedback.
d. Implement reporting and auditing procedures to ensure that the CSIRT is performing efficiently and meets established service level agreements or performance metrics.

Common problems: no methods are instituted for evaluating whether the CSIRT is accomplishing its mission; methods for process improvement are not implemented; performance metrics do not adequately measure CSIRT performance.

18) Have a backup plan for every element of the CSIRT.

a. Identify key and critical CSIRT functions, services, and equipment.
b. Design a disaster recovery and business continuity plan for critical CSIRT services and processes; these plans should tie into similar plans for the parent organization.
c. Plan what will happen if someone cannot fulfill their role or cannot provide space or equipment needed by the CSIRT.
d. Institute mock exercises to test whether CSIRT functions and facilities can be operational during emergency situations.

Common problems: the CSIRT has no reach-back[5] capability ready if additional staffing is needed during peak or emergency situations; key CSIRT systems and networks that provide critical functions and services are not backed-up, resulting in the CSIRT not being able to function during an emergency situation.

19) Be flexible.

a. Do not try to do too much at once. However, be ready to adapt and take advantage of good opportunities when they arise; if such opportunities will not severely tax the CSIRT resources and cause problems delivering existing CSIRT services.
b. Understand that services may evolve over time and be ready to learn new skill sets and gain new knowledge.
c. Keep learning about changing technologies to ensure response strategies are

effective for dealing with new threats and risks.

d. Look for ways to collaborate with others in the CSIRT and security fields.

CSIRT Resources

Handbook for Computer Security Incident Response Teams
http://www.cert.org/archive/pdf/csirt-handbook.pdf

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

Organizational Models for CSIRTs
http://www.cert.org/archive/pdf/03hb001.pdf

State of the Practice for CSIRTs
http://www.cert.org/archive/pdf/03tr001.pdf

Steps for Creating National CSIRTs
http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

Defining Incident Management Processes
http://www.cert.org/archive/pdf/04tr015.pdf

Staffing Your CSIRT
http://www.cert.org/csirts/csirt-staffing.html

Footnotes

[1] A “stakeholder” is any individual or group with an interest in the success of the CSIRT and its mission. Stakeholders can be those who will report to the CSIRT, receive help from the CSIRT, provide funding and sponsorship to the CSIRT, or interface with the CSIRT through information sharing or the coordination of incident and vulnerability handling activities.

[2] The “constituency” are the people or organizations serviced or supported by the CSIRT.

[3] “Compliance” refers to making sure the CSIRTs policies or procedures agree with applicable laws or policies that are in place organizationally, locally, nationally, or internationally. For example, in the U.S. there are many state laws that require companies to notify customers if their personal data is released without their consent or authorization. If a CSIRT in a state with such laws is tasked with handling computer security breaches, it (or its parent organization) must comply with the law regarding any required notification.

[4] “Mission creep” refers to a situation in which a CSIRT begins to perform activities outside the scope of its mission or defined purpose and function.

[5] Reach-back capability is the ability to call in additional staff outside your normal CSIRT staff during peak times. For example, if you are using a contractor to supplement CSIRT staff and a major incident occurs, a reach-back capability would allow the contractor to call in more people to help handle the incident. In this case the contractor would “reach back” into their total pool of employees to temporarily supplement the CSIRT staff until the incident was resolved and operations returned to normal. If a CSIRT does not have contractors providing staff, then reach-back might be handled by pulling people from other parts of the organization to help until the incident was resolved.

Top

Last updated October 18, 2006