Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

Steps for Creating National CSIRTs

August 2004

Georgia Killcrece
CERT CSIRT Development Team
CERT® Coordination Center
Networked Systems Survivability Program
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
USA

Acknowledgements

I would like to extend my personal thanks to Robin Ruefle and Mark Zajicek, my fellow teammates on the CSIRT Development Team, who participated in the development and reviews of this white paper. My thanks also go to Jeffrey Carpenter, Technical Manager of the CERT® Coordination Center, and the Organization of American States, who supported the development of this work.

I would also especially like to express my thanks to colleagues in the CSIRT community who gave of their time to help improve the clarity of the content contained in this document:

- Henk Bronk of the Netherlands GOVCERT.NL
- Cristine Hoepers of the NBSO/Brazilian CERT
- Robert Wayne Mead of the Australian response team, AusCERT
- David Parker and Andrew Powell from the UK National Infrastructure Security Co-ordination Centre, NISCC

Each of my colleagues above has provided thoughtful discussion, insightful comments, and suggestions to further refine the quality of the material. Much of what we know today is based upon the past experiences of the CERT/CC and efforts of many other members of the global CSIRT community. That body of knowledge and their input are much appreciated.

Purpose of This Document

This purpose of this document is to provide a high-level description of a Computer Security Incident Response Team (CSIRT), the problems and challenges facing these CSIRTs, and the benefits for developing such a team or response capability at a national level.[1]

The need for action to mobilize the global community and develop national capabilities is clear. When widespread cyber events occur, it is critical that mechanisms are in place to

- effectively detect and identify the activity
- develop mitigation and response strategies
- establish trusted communications channels
- provide early warning to affected populations and constituencies
- notify others within the internet and security communities of potential problems
- effect a coordinated response to the activity
- share data and information about the activity and corresponding response solutions
- track and monitor this information to determine trends and long term remediation strategies

This document also describes the basic steps that can be used for building a CSIRT, the issues and tasks to be addressed when planning and implementing such a team, and the coordination that is needed between such teams to provide effective analysis and response to cybersecurity incidents.

Introduction

Many governments, business enterprises, academic institutions, and individuals are using the dynamic and inter-connected environment of today's networked information systems to improve communications, provide control, protect information, and encourage competitiveness. In many cases, the low cost of communications via the internet is replacing other traditional forms of communications (such as paper-based communications and the telephone). Computers have become such an integral part of business and government that computer-related risks cannot be separated from general business, health, and privacy risks. Valuable government and business assets are now at risk over the internet. For example, customer information may be exposed to intruders. Financial data, intellectual property, and strategic plans may be at risk. The widespread use of databases leaves the privacy of individuals at risk. Increased use of computers in safety-critical applications, including the storage and processing of medical records data, increases the chance that accidents or attacks on computer systems can cost people their lives.

[1] The CERT Coordination Center and the CSIRT Development Team, who provided much of the impetus for the development and evolution of this body of information to help others create their teams is gratefully acknowledged. In addition, appreciation and thanks are extended to colleagues in the CSIRT community who graciously provided reviews and insight into some of the nuances of language and other national team planning and development issues.

The internet itself has become a critical infrastructure[2] that must be protected. It continues to expand[3] and there is a continuing movement towards distributed, client-server and heterogeneous configurations. As the technology is distributed, it is often the case that the management of the technology is distributed as well.

Our overall reliance on the internet continues to increase. Unfortunately, in this dynamic, distributed, and interconnected environment cyber attacks occur rapidly and can spread across the globe in minutes without regard to borders, geography, or national jurisdiction. As a result, there is a growing need to be able to communicate, coordinate, analyze, and respond to cyber attacks across different business sectors and national borders.

Background

The need for a community of computer security incident response teams was recognized in the late 1980's when the Defense Advanced Research Projects Agency created the Computer Emergency Response Team Coordination Center at Carnegie Mellon University's Software Engineering Institute. Chartered to respond to security events on the internet, the CERT/CC was also chartered to serve as a model for the operation of other response teams and to foster the creation of additional teams, each focused on meeting the needs of a particular constituency. Even then it was clear that the diverse technologies, constituencies, global demographics, and breadth of services needed by these constituencies could not be provided by any single organization. No one team would ever be able to effectively respond to all attacks against computer networks or network connected systems – the problem would become too large, the technical knowledge required too broad, the user constituencies needing help too diverse, and the likelihood of developing universal trust too small. Currently, there is no over-arching infrastructure to globally support a coordinated incident response effort; although there are efforts underway to develop cooperative relationships that support such a capability.

Today there are several hundred CSIRTs serving a variety of commercial, academic, government, military organizations.[4] For the most part they are focused on and provide services and support to their defined constituency for the prevention of, handling, and response to cybersecurity incidents. Many of these teams are focused on the technical aspects of cybersecurity incidents and coordinating cross-sector initiatives to solve these incidents. It is important to note that these CSIRTs do not replace existing national and local emergency preparedness, disaster recovery, business continuity or crisis teams, nor do they replace other national policing or intelligence agencies.

[2] Critical infrastructures are those essential services and support functions that are necessary to ensure operations of a government or economy. They include, for example, telecommunications, critical government information systems, food and water supplies, transportation, power and electric generation, oil and gas production, banking and financial systems, and health and emergency services.

[3] The January 2004, the Internet Domain Survey, from ISC, reported 233 million hosts advertised in the domain name service <http://www.isc.org/index.pl?/ops/ds/>.

[4] Appendix A contains a reference map of incident response teams around the world. Many of these teams are members of the Forum of Incident Response and Security Teams, a coalition that brings together a variety of computer security incident response teams from government, commercial, and academic organizations, see <http://www.first.org>.

They may interact or provide technical expertise to help with law enforcement investigations, intelligence operations, or political activities, but it is not their core CSIRT mission. To the extent that it is appropriate and logical to do so, they can develop relationships with these other entities to facilitate communications when cybersecurity incidents are involved or if there is a need for coordination at a national/country level.

Various national[5] and regional[6] initiatives are being implemented to strategically address the protection of key resources and critical infrastructures, as well as to build a community of CSIRTs. Some of the goals of these national and regional initiatives include

- establishing a national focal point within a country or region to coordinate incident handling activities
- analyzing and synthesizing incident and vulnerability information disseminated by other teams, vendors, and technology experts to provide an assessment for their own constituency and communities
- facilitating communications across a diverse constituency—bringing together multiple sectors (government and military, critical services and infrastructures, commercial, academic, banking and finance, transportation, etc.) to share information and address computer security problems, such as widespread computer security incidents, threats and vulnerabilities.
- developing mechanisms for trusted communications within these communities

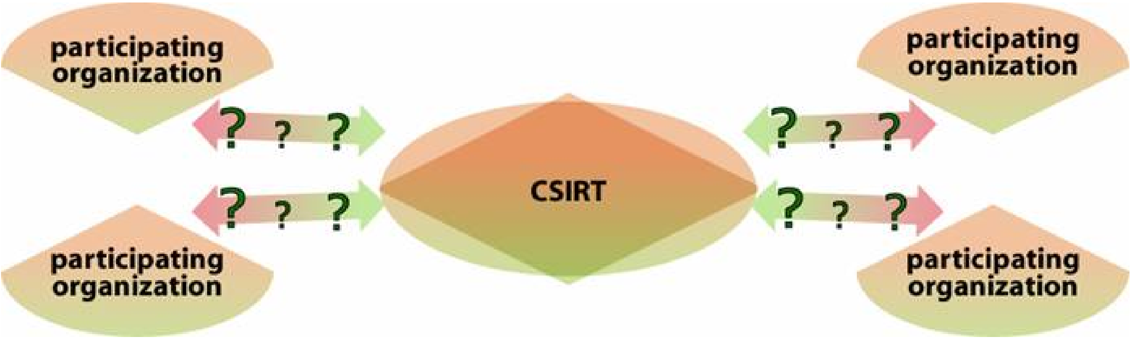
In other locations, governments have recognized the need for developing and implementing an incident response capability to address cybersecurity problems—in some cases, government mandates or other regulatory requirements have been established ***requiring*** these capabilities be created and requiring them to report annually on information security issues (e.g., the U.S. Federal Information Management Act of 2002).[7] Government organizations now understand the importance and challenges in protecting not only their information but the critical infrastructures that support the economies within their borders. They are seeking effective and coordinated approaches to respond to cyber incidents, threats and attacks that can cross public and private sectors. They also recognize the need to facilitate interaction both at the domestic and international levels, and be a focal point for reporting cybersecurity events, coordination, and communications.

A few teams with national responsibilities are also beginning to participate in global "watch and warning" efforts to secure cyberspace.

[5] For example, in 2004 The Comprehensive Risk Analysis and Management Network (CRN) published the *International CIIP Handbook 2004*. This handbook provides overviews of the protection strategies for a number of country-level efforts. The full report is available from <http://www.isn.ethz.ch/crn/publications/publications_crn.cfm?pubid=224>.

[6] See <http://www.ti.terena.nl/> and <http://www.apng.org/old/archive/wg-charter/apng-apsirc.html>.

[7] See <http://www.fedcirc.gov/library/legislation/FISMA.html>


participating organization
participating organization
participating organization
participating organization
? ? ?
? ? ?
? ? ?
? ? ?
CSIRT

From another perspective, a national-level (or government-sponsored) CSIRT can also serve as the “response team of last resort” – that is, if a cybersecurity incident needs be reported and it is unclear where it should be reported, it can be reported to this national or country-level CSIRT; who will either redirect to the appropriate response team for handling or will provide some minimal level of support.

The Problems and Challenges

A growing number of government, commercial, and educational organizations depend on computers to such an extent that day-to-day operations are significantly hindered when the computers are “down” or inaccessible. Use of the internet enhances the ability of organizations to conduct their activities in a cost-effective and efficient way. But these and other critical infrastructure operators are concerned that their computer systems are vulnerable both to attack and to being used to further attacks on others. In addition, there are still many places where no team exists or where incident response occurs in an *ad hoc* fashion.

The internet is complex and dynamic, but among those connected to the internet there is a lack of adequate knowledge about the network and security—for example, misconfigured or outdated operating systems, vulnerabilities in software, unpatched systems, and a lack of security awareness by individual users provide a rich environment for intruders to exploit. It is easy to exploit the many security holes in the internet and in the software commonly used in conjunction with it; and it is easy to disguise or hide the true origin and identity of the people doing the exploiting. Moreover, the internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries.

The need for developing a community of educated, trained, knowledgeable, and aware practitioners who understand the risks and issues related to cybersecurity incidents and the threats and attacks from vulnerabilities has never been clearer than it is today.

Benefits National Teams Can Provide

From a technical security standpoint national teams can

- serve as a trusted point of contact
- develop an infrastructure for coordinating response to computer security incidents within a country or economy, e.g., for incident and threat activity related to any potential national risk(s) to its critical infrastructures, and on any perceived trends regarding future attacks and their precursors
- develop a capability to support incident reporting across a broad spectrum of sectors within a nation's borders
- conduct incident, vulnerability, and artifact analysis and to
  - disseminate information about reported vulnerabilities and corresponding response strategies
  - share knowledge and relevant mitigation strategies with appropriate constituents, partners, stakeholders and other trusted collaborators. (This may also include coordination with vendor communities).
- participate in cyber "watch" functions; encourage and promote a community of national and regional teams that share data, research, response strategies, and early warning notifications with each other and with similar points of contact throughout their own critical infrastructures and more broadly beyond their national borders.
- help organizations and institutions within the nation develop their own incident management capabilities (e.g., provide guidance and information for planning and implementing the teams, build relationships and stimulate discussions among and across these government agencies, public/private businesses, or academic organizations). This may also lead to developing baselines and benchmarking methods or evaluating the capabilities of these teams. This might also include a mechanism for certifying or accrediting CSIRT organizations with their country or economy.
- provide language translation services for technical analyses of malicious code and other computer security information from external entities
- make general security best practices and guidance available through publications, web sites, and other methods of communication. (This type of information can include technical guidance for securing host and network configurations, links to other trusted resources and information for implementing secure communications systems, or helping individual users protect their systems.)
- promote or undertake the development of education, awareness and training materials appropriate for a variety of different audiences. Target populations can include system and network administrators, other organizational CSIRTs within the country's borders, policy makers, legal representatives, law enforcement and/or regulatory agencies, and general user populations.
- identify and maintain a list of CSIRT capabilities and points of contact within a country or economy.

In addition to the above, national teams can coordinate with other national-level teams to leverage trusted experts who can provide further technical insight into security incidents and vulnerabilities. Additionally (where local teams typically may not have these capabilities) national-level teams can liaise with other governmental authorities on matters that could affect critical infrastructures or broader national security matters.

Globally, CSIRTs will focus on important key issues, such as developing infrastructures and mechanisms that enable trusted communications channels and that quickly facilitate the coordination of alerting and response actions. They are interested in using existing capabilities where it makes sense to do so for building resilient infrastructures that can deliver essential services and preserve essential assets during attacks and compromises, as well as to recover the services and assets after attacks—without compromising the mission. They recognize that new systems and applications being deployed or repurposed must be more secure and implement authentication, transport, and access control mechanisms—and integrate information technology security improvements that provide ease of use as well as ease of administration.

They also want to leverage existing training and educational programs to develop, enhance, and further improve the skills and technical knowledge of CSIRT staff, information technology staff, and network security personnel (and other relevant stakeholders) within their constituencies.

Activities and topics, such as those mentioned above, must be discussed and resolved within multiple teams, not only within an organization or enterprise, but regionally, nationally, and within those teams who operate internationally. The speed with which such threats can be recognized, analyzed, and responded to will minimize the damage and lessen the costs of recovery.

However, as mentioned earlier, many organizations do not have a formalized CSIRT or incident management capability in place; they lack a repeatable or comprehensive set of processes for handling computer security incidents.

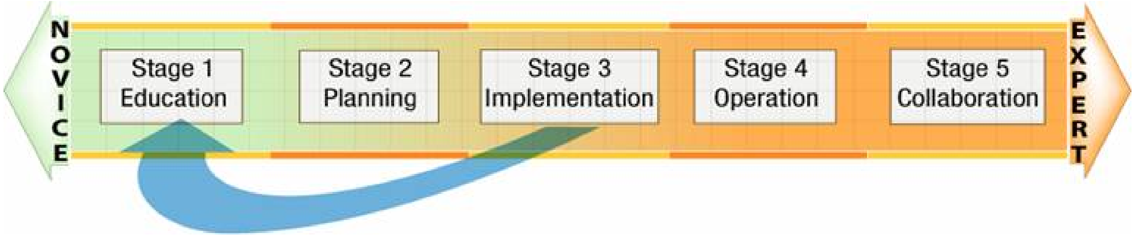
Similarly, at national levels, gaps in incident response, management, and coordination processes mean that some nations are more at risk than others. Some may lack adequate staff and resources to effectively monitor such activity, protect critical services and supporting networks, and respond to incidents that affect critical infrastructure services (including those in the financial, educational, health, energy, government, and military sectors). Without having a clear understanding of the underlying security issues, or a defined plan for coordinating response efforts, they face the risk of exposure of sensitive data, financial losses, and potentially the loss of life.

To begin to address these concerns, and provide some tangible guidance that can help, the following sections describe a high-level set of steps that can be used to create a CSIRT.

High-Level Steps for Creating a CSIRT

In experiencing the development of our own team and observing how other teams have formed and evolved over time, the CERT/CC has identified a set of basic “stages” that a newly forming team moves through. These stages describe the development from the initial thoughts about having a team through its fully operational capability as a CSIRT.

Although each team may differ in how it operates on a day-to-day basis, all will exhibit these characteristics during their development processes.



The high-level stages provide a way of understanding what is involved in creating a team; from planning to building and sustaining an incident management capability. Some of the steps include identifying key stakeholders and participants in the development process; developing a strategic plan and vision for how the CSIRT will be organized, structured, staffed and funded; training the CSIRT staff to operate the CSIRT; and incorporating mechanisms to evaluate and improve CSIRT operations.[8]

Often teams (both new and more mature) realize that as they cycle through a stage, there is additional information they may need to find out and they must go back to an earlier stage and do additional work. For example, once the team is operating, new staff may be hired who need to be trained or educated to understand the roles and responsibilities of the team. Or, a change in the constituency may require a change in the mission, goals or objectives of the CSIRT, which could mean developing new plans. New funding and expansion of the team may change how the services are implemented. This can result in a return to the planning stage or other stages..

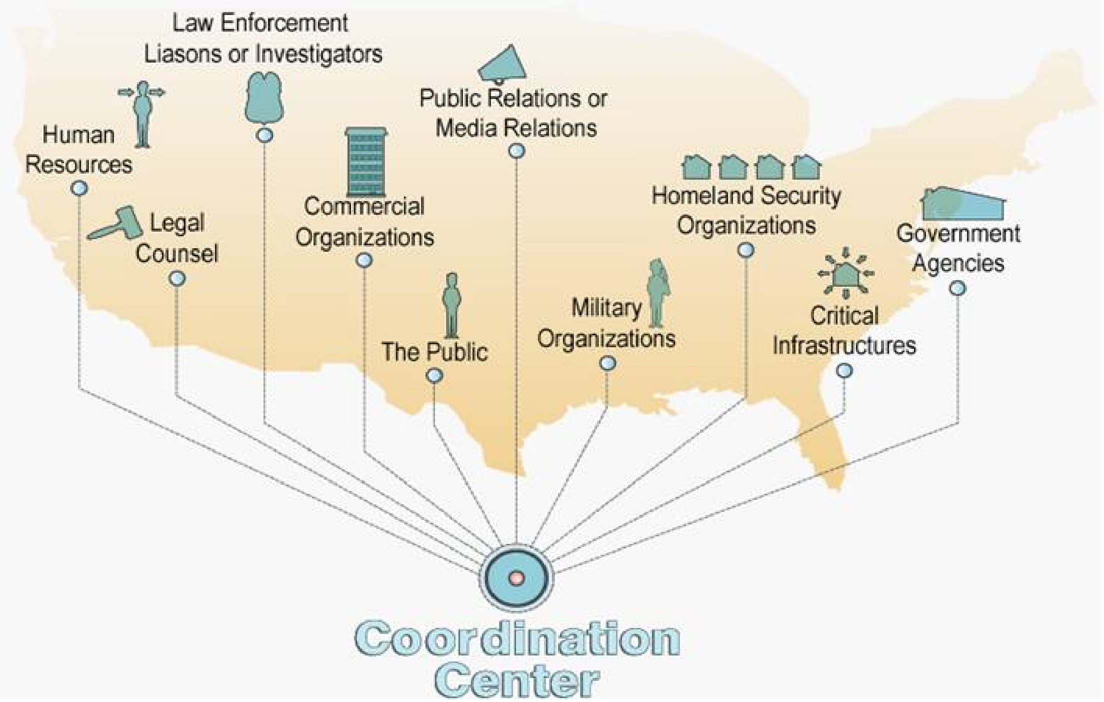
In the next several sections, each of these stages (Education, Planning, Implementation, Operation, and Collaboration) is described in more detail to provide a starting place that can be used by those who are tasked with creating a national-level team.

Stage 1 – Educating stakeholders about the development of a national team. This is an awareness stage, where those who need to participate in and promote or “champion” the development and promotion of a national incident response capability learn what is involved in establishing the CSIRT—the decisions that must be made, the role the CSIRT will play (e.g., as a national focal point for incident reporting and response), and the key issues that are likely to be faced (management and staffing, developing trusted communications and coordination, effective processes, etc.)

[8] For general information on creating a CSIRT, see the *Handbook for CSIRTs, 2nd Edition,* available at <http://www.cert.org/archive/pdf/csirt-handbook.pdf> and *Creating a CSIRT, A Process for Getting Started* at <http://www.cert.org/csirts/Creating-A-CSIRT.html>.

In addition to leveraging publicly available training on CSIRT development issues, meetings and facilitated discussions should occur to raise issues related to establishing a national CSIRT capability and the benefits such an entity will provide. Such meetings and discussions should include, for example:

- understanding the business drivers and motivators behind this need for a national team (applicable regulatory requirements, critical infrastructures to be protected, the types of incidents or attacks that are occurring and that affect national interests, etc.).
- understanding what is involved in developing incident response capabilities at a national team level (e.g., regulatory and legal requirements, determining who the constituency will be, mobilizing and staffing the team, outlining resource and infrastructure requirements, obtaining funding, developing partnerships, establishing security policies and guidelines).
- identifying the people to be involved in the discussions for building a national team, those who will be involved in developing and promoting the CSIRT, and those who need to be involved in the planning and implementation process. This might include selected representatives from government agencies, critical infrastructures, homeland security organizations, military organizations, industry partners/commercial organizations, local and organizational CSIRTs or security teams, technology vendors, security product vendors, trusted experts, policy/law makers, legal counsel, human resources, public relations or media relations, law enforcement liaisons, business managers, IT and telecommunications staff, etc.
- learning what key resources and critical infrastructures exist within the nation
- identifying the types of communications channels that need to be defined—not only for coordination during the development process, but later, for communicating across the participants involved in the CSIRT constituency
- considering the types of high-level mission, goals, objectives, and expectations a national team might establish.
- determining the specific laws, regulations, and other policies that will affect the national CSIRT development (what constraints, level of authority, information protection, or compliance issues will determine its operation)
- investigating and identifying funding strategies that can be used to develop, plan, implement and operate the response capability
- determining technology and network information infrastructures that will be needed to support the operations of the national team
- discussing basic response plans and interdependencies as they apply across a variety of sectors (government, business, finance, education, etc.)
- understanding the potential set of core services that a national CSIRT may provide to its constituency
- reviewing and researching what other countries are doing to create their national teams and identifying any best practices or guides that can be applied to this development effort



Stage 2 – Planning the CSIRT. Building on the knowledge and information that is gained during Stage 1; the next steps are to design and plan the national CSIRT. Issues that are reviewed and further discussed during this stage will include articulating the need for having a team and benefits it will provide, identifying its constituency, the services and support (or "role") the national CSIRT will have, determining estimated costs to create and operate the team, a timeframe for putting it in place, the people who will be tasked with taking the plan and moving it forward towards implementation and operation of the CSIRT.

More specifically, activities at this stage include

- outlining the requirements and need for the national CSIRT.
  This will include collecting information specific to the national CSIRT regarding
  - laws and regulations that will affect operations of the national team
  - critical resources that need to be identified and should be protected
  - current incidents and trends that are being reported or should be reported
  - existing incident response capabilities and computer security expertise
  - gaps in providing coordinated response across the nation
- developing a vision for how the national CSIRT will operate.
  This will include
  - defining the mission of the national team
  - determining the constituency (or constituencies) that it will serve
  - identifying the communications interfaces between the constituency and the national team (what exists and what will need to be developed or modified)
  - determining the set of services that should be provided (e.g., alerts and announcements, translation services, incident analysis, incident response coordination, vulnerability analysis and coordination, evaluation of other teams

within the nation state through assessments or benchmarking, security awareness training, etc.[9])

  - identifying the organizational model, authority, and physical location for the national team, as well as the local protection requirements
  - identifying the staff, equipment, and infrastructure needed to support and sustain the CSIRT
  - developing budgets and funding proposal, project plans, or business operations plans. Funding strategies, for example, could include fee-based services, contract services, government sponsorship, academic or research sponsorship, consortium sponsorship, membership subscriptions, or some other combination of funding sources. In addition to initial start-up funding (that cover staff, space requirements, equipment and infrastructure costs, operational costs, etc.), budget plans for long-term sustainment of the CSIRT should also be prepared.

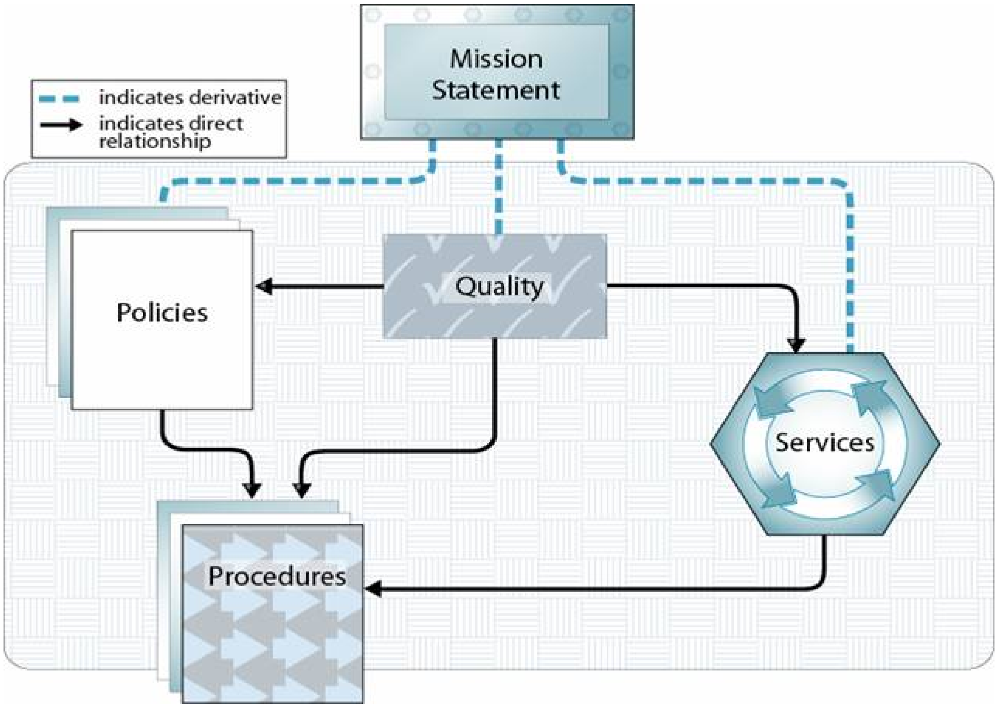
- identifying the type of national (government) approval, leadership, and sponsorship that is needed for the CSIRT to be successful—and obtaining that support
- identifying the types of staff skills[10] and knowledge that is needed to operate the team
- defining the types of roles and responsibilities[11] for the national CSIRT (and the specific tasks to be undertaken, by whom, when, and under what conditions, the type of recording and tracking required, etc.)
- specifying the incident management processes the team undertake (e.g., what will they do for prepare, protect, detect and response functions) as well as determining the relationships to similar processes in any of the external constituent organizations
- developing a standardized set of criteria and consistent terminology for categorizing and defining incident activity and events
- defining a set of incident handling guidelines, reporting requirements, and forms to outline how the national CSIRT will interact with the constituency and other global CSIRTs or external partners
- determining any needed processes for integration with existing disaster recovery, incident response plans, business continuity plans, crisis management or other emergency management plans
- identifying any constraints that might affect the development process and planning mitigation strategies (this could relate to compliance issues, infrastructure, or other political or socio-economic conditions)
- determining methods for building trusted relationships and collaboration agreements with other key resources and critical infrastructures
- designing the communication and coordination processes and mechanisms for information dissemination to the national CSIRT's constituency (e.g., email, websites, published reports, or other mechanisms)

[9] See the List of CSIRT Services for information about a range of services that a CSIRT might provide. It is located at <http://www.cert.org/csirts/services.html>.

[10] Appendix B contains a list of some of the basic skills that members of the CSIRT should have (or have access to personnel with those sets of skills).

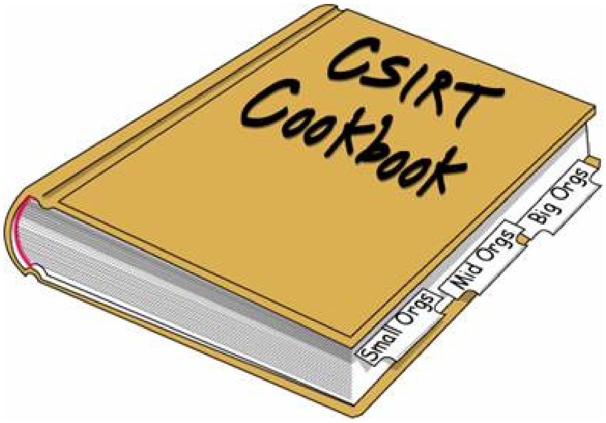
[11] See Appendix C for a list of CSIRT roles and position descriptions.

- developing project timelines, deliverables
- creating the national CSIRT plan based on outcomes from the planning activity, the vision and corresponding framework; obtaining feedback and review of the plan, incorporating revisions to the plan as necessary, developing schedules for reviews and modifications of the planning document and other supporting materials



The planning team may also want to develop a concept of operations document to assist in scoping or bounding the responsibilities of the team. Such a document would become the roadmap for development or the “vision” of the CSIRT and would capture the high-level overview of the above bulleted items (such as articulating or explaining the mission, goals and objectives, the constituency being served, authority, organizational structure and location of the team, set of services provided, etc.). It would also include information about guiding principles and other regulatory considerations, the coordination roles and responsibilities, how it will interact with others, the expectations and reporting requirements or guidelines, and discuss the structure and types of relationships the team has with other organizations (e.g., internal and external entities).

- **Stage 3 – Implementing the CSIRT**. During this stage, the project team uses information obtained from the previous two activities to build and implement the national CSIRT.



The basic steps that are involved include

- getting the funds (from sources identified during the planning stage). In this implementation stage, it means actually procuring or arranging that the funds are obtained or made available.
- announcing broadly that a national CSIRT is being created and where additional information can be obtained (about the team, rationale for developing the capability, progress on the development, reporting requirements, etc.)
- formalizing coordination and communications mechanisms with stakeholders and other appropriate contacts (identifying the process for establishing points of contact, any formal requirements for non-disclosure or required information sharing[12] agreements, encryption standards, or information dissemination guidance and corresponding procedures, etc.)
- implementing the secure information systems and network infrastructures to operate the national CSIRT (e.g., secure servers, applications, desktops, telecommunications equipment and other infrastructure support resources).
- developing operational policies and procedures for the CSIRT staff, including the criteria and reporting guidelines agreed to in the planning stage.
- developing internal policies and procedures for access and operation of CSIRT equipment and personal equipment, as well as acceptable use policies
- implementing processes for the national CSIRT's interactions with its constituency
- identifying and hiring (or reassigning) personnel, obtaining appropriate training and education for the CSIRT staff, as well as determining other potential outreach efforts to train and educate the constituency

[12] Information sharing in this context is related to details about specific cybersecurity incidents, software vulnerability information, malicious code, etc. that is used or needed in incident response operations.

Stage 4 – Operating the CSIRT. At the operational stage, the national CSIRT has a basic incident management capability in place and the team is actively receiving incident reports and coordinating responses to incidents. It is operational.

The tasks identified in the planning and implementation stages now have form and substance. The national CSIRT has a vision with a framework that defines the mission, goals and objectives, structure, authority, funding, resources, and infrastructure to support and sustain the team.

Policies and procedures have been developed and implemented; including methods for developing and maintaining trusted relationships with partners, processes for establishing protected communications channels, plans for coordinating response and analysis functions, approaches for developing mitigation strategies, and disseminating information to the appropriate constituencies.

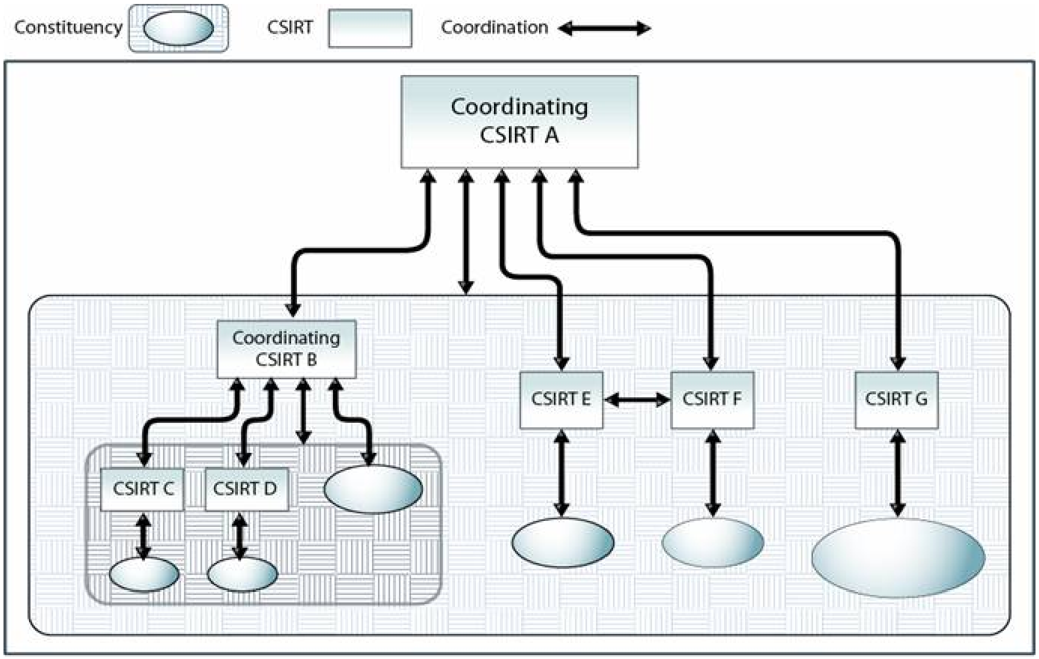
Key stakeholders and other constituencies (CSIRTs and trusted experts) recognize the team and the services and support provided by the national team.

Clearly defined procedures for communications, coordination, and escalation in responding to cyber threats and preventing attacks are implemented and sustained.

The national team promotes the development and implementation of other local CSIRTs within its borders through resources such as documents, plans, templates for procedures and guidelines, training and awareness information, and other resource materials (possibly through a publicly accessible website).

Tasks occurring at this operations stage include

- actively performing the various services provided by the national CSIRT
- developing and implementing a mechanism for evaluating the effectiveness of the national CSIRT operations. This allows the national team to evaluate its operational capability to ensure it is meeting its mission and goals, as well as the needs of the community
- improving the national CSIRT according to the results of the evaluations
- expanding the mission, services, and staff as appropriate and as can be sustained to enhance service to the constituency (e.g., providing language translation services, expanded analysis and research capabilities)
- continuing to track any changes in the constituency, legislation, policy, or other regulations that will affect the overall mission and goals of the national team and determining mechanisms for implementing and incorporating changes in its operations to improve its effectiveness
- training new and existing staff in the national CSIRT's operations, incident handling processes and procedures, attack trends, mitigation strategies, and tools, and general information assurance knowledge as needed (this might include providing professional development and continuing education opportunities for appropriate staff)
- continuing to develop and enhance CSIRT policies and procedures



Stage 5 – Collaboration. As the national CSIRT continues its operations and refinements, in parallel it is also maturing—it is further developing trusted relationships with key stakeholders, partners, and other CSIRTs. This mature team has been in existence for a period of time and has extensive experience in incident handling and management activities. It is a trusted partner in the global CSIRT community.

The team has institutionalized its operations in the detection of cyber threats, response and the remediation of problems.

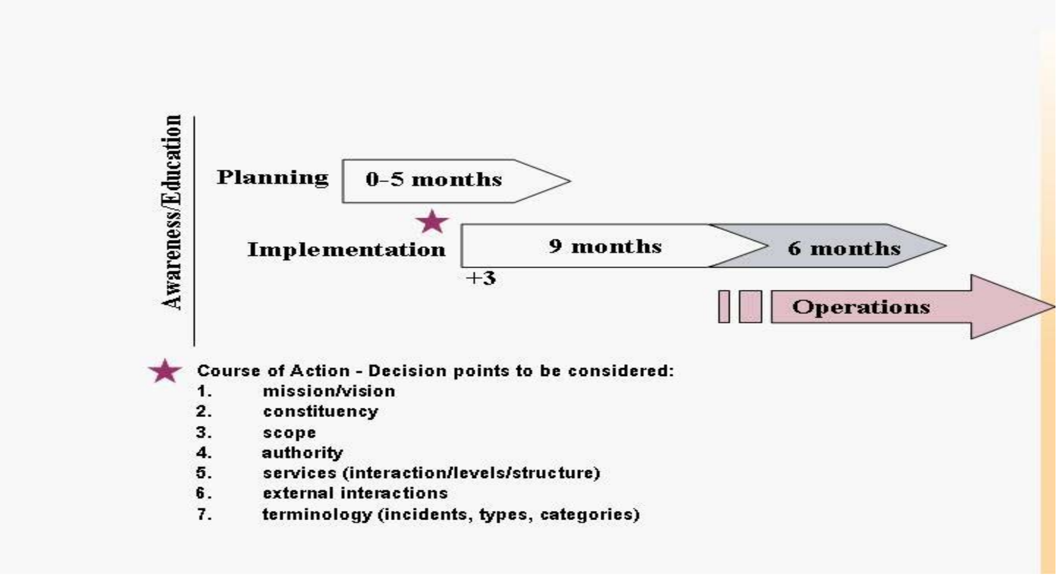
Activities at this stage include:

- participating in data and information sharing activities and supporting the development of standards for data and information sharing between partners, other CSIRTs, constituents, and other computer security experts
- participating in global "watch and warning" functions to support the community of CSIRTs

- improving the quality of CSIRT activities by providing training, workshops, conferences that discuss attack trends and response strategies
- collaborating with others in the community to develop best practice documents and guidelines for protecting and securing critical infrastructures and for developing response strategies and plans
- reviewing and revising the processes for incident management as part of an on-going improvement process. Changes in services provided by the CSIRT or other operational activities are announced broadly to the constituency and other stakeholders as appropriate.
- promoting the development of organizational CSIRTs within the nation's constituency and serving as a role model in the development of best practices for these newly developing CSIRTs. The national team may also provide services to evaluate and benchmark (or even certify and accredit) these CSIRTs.

Timeline

From initial education and awareness to peer collaboration will take time, especially when relating to the development of a national capability. Depending on the resources that are provided and "buy-in" from its key stakeholders and constituency, a CSIRT can take anywhere from 18-24 months to become fully operational (see the projected timeline below). This timeline can be extended or compressed, depending on a number of factors and decision points that are made. These are indicated at the bottom of the picture. The amount of resources that are available to define the mission, goals, and scope, etc., of the team will determine how quickly the CSIRT project can move from initial inception through planning and into the implementation and operations stages. As can be seen in the graphic, there are possibilities for overlapping some of the implementation and operational components (depending on progress of the project planning and implementation).



Note: This timeline focuses on the first four stages of development (discussed earlier in the document, on page 9). It does not include maturation into the “collaborative” phase (Stage 5) of development; although during operational activities, the team will begin to build the trusted relationships that will lead to such collaborative activities.

In many cases, teams will start with a small number of services that they can provide (e.g., perhaps just a centralized point of contact for cybersecurity incidents or coordination of responses, or a clearinghouse for disseminating computer security information resources), then gain acceptance from the community and begin to add additional services and support as resources permit. In this way the team builds the trust, respect, and understanding from the constituency it serves by proving it can be effective.

Training and education requirements will need to be scheduled to support the activities of the team (e.g., for new staff, project managers, incident handlers, analysts, support and other administrative staff who oversee and operate the national CSIRT). These training and mentoring activities can affect the range as well as the level of services that are implemented and provided to the constituency.

For the team to succeed, it is important to have strong commitment to and management of the project throughout all the stages of development, as well as to have long-range plans to sustain and operate the team over time.

Conclusions

Internet security has become increasingly critical to the stability and well-being of the every internet-connected organization and nation. Our critical information infrastructures and the government and business operations that depend on the internet are at risk. We share the responsibility to improve internet security and coordinate effective international global response to cybersecurity incidents and events.

To be successful, it is paramount that coordination and cooperation occurs among governments, law enforcement, commercial organizations, the research community, and practitioners who have experience in responding to IT security incidents; and that it continues to expand and improve. National CSIRTs can play an important role by helping their internet-connected sites protect their systems, detect, recognize, and analyze compromises to the security of those systems, protect themselves from malicious activities, and when cybersecurity incidents occur, quickly and effectively coordinate and respond to attacks. These teams can also be evangelists in promoting and helping other organizations within their national borders build effective incident management capabilities.

What is clear and what we continue to hear from our partners in the CSIRT community is captured by the following statements:

- less time to react
- need for quick notification
- need for automation of incident handling tasks
- need an easy way to collaborate and share information with others
- need an easy and efficient way to sort through all incoming information
- required policies and procedures must be established and understood

Trustworthiness is paramount to success

A team will live or die by its credibility –if the constituency stops trusting in the CSIRT then it will be next to impossible for it to succeed. It takes time to promote and gain the constituency's acceptance and trust of the CSIRT, its role, and the products and services it provides.

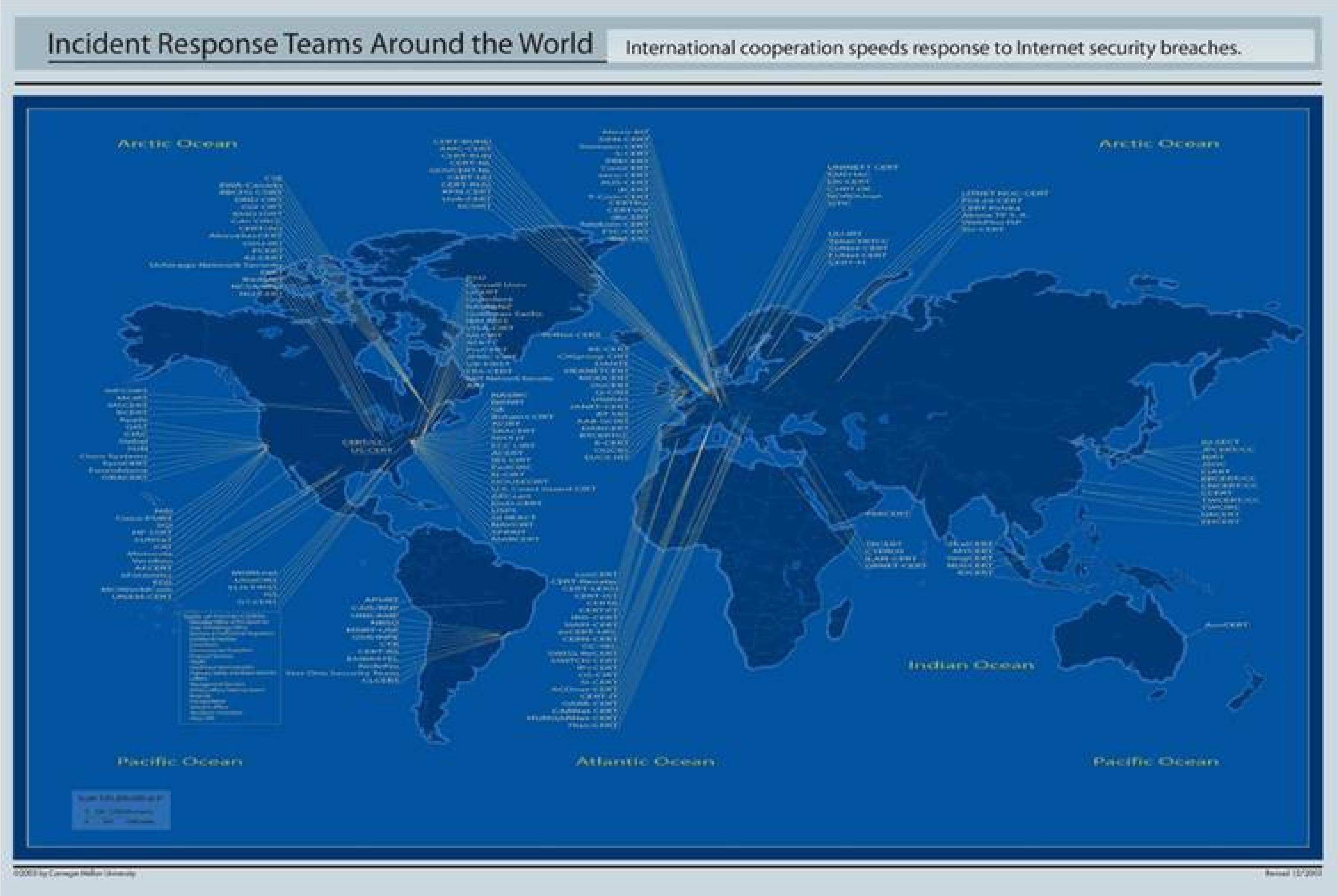
Once recognized as a source of help, the CSIRT will need to focus on its guiding principles and the rules under which it operates so that the team, management, constituency and other CSIRTs understand how the CSIRT is (or is not) able to assist or work with them..

Even if a team has no direct authority over its constituency (especially true in the case of a national CSIRT), it can still be successful—by winning the trust, respect and understanding of others with whom it interacts and through setting the correct expectations for the goals and objectives of the team. It is also important to understand that every team is different based on its mission and the needs of its constituency.

Finally, CSIRTs should

- share information as openly as possible
- set expectations repeatedly
- train for a marathon, not a sprint
- be proactive

Appendix A: CSIRTs Around the World


Incident Response Teams Around the World
International cooperation speeds response to Internet security breaches.
Arctic Ocean
Arctic Ocean
Indian Ocean
Pacific Ocean
Atlantic Ocean
Pacific Ocean

Appendix B: Basic Staff Skills

The composition of CSIRT staff varies from team to team and depends on a number of factors, such as

- mission and goals of the CSIRT
- nature and range of services offered
- available staff expertise
- constituency size and technology base
- anticipated incident load
- severity or complexity of incident reports
- funding

Many teams possess a core group of individuals who provide the basic level of incident handling services. Each CSIRT staff member is expected to have some minimum set of basic skills to do the work and be effective in their work responsibilities. Listed below is a set of basic staff skills that CSIRT staff should possess to be effective in their work.[13] For more detailed descriptions of these skills

Personal Skills

a) communication skills (oral and written)
b) diplomacy
c) ability to follow policies and procedures
d) ability to work as a contributing member of a team
e) integrity
f) knowing one’s limits
g) ability to cope with stress
h) problem solving
i) time management
j) attention to detail

Technical Skills

a) good technical foundation
b) security principles
    i) authentication, integrity, confidentiality, authorization, privacy, non-repudiation, access-controls
c) security vulnerabilities and weaknesses
    i) physical security
    ii) protocol design flaws
    iii) implementation flaws (e.g. buffer overflow)

[13] For more detailed descriptions, see "Staffing Your Computer Security Incident Response Team – What Basic Skills are Needed?” <http://www.cert.org/csirts/csirt-staffing.html>.

  iv) configuration weaknesses
  v) user errors/indifference
  vi) malicious code (e.g. viruses, worms, Trojan horses)
d) Internet history and evolution
e) computer security risks
  i) lose of life, reputation, money, services
f) network protocols (purpose, specification, operation)
  i) IP (Internet Protocol)
  ii) TCP (Transmission Control Protocol)
  iii) UDP (User Datagram Protocol)
  iv) ICMP (Internet Control Message Protocol)
  v) ARP (Address Resolution Protocol)
  vi) RARP (Reverse Address Resolution Protocol)
g) Domain Name System (DNS)
h) network services and applications
i) defensive security measures
j) host/system security issues and measures
  i) secure configurations
  ii) available tools
k) understanding and identifying intruder techniques
l) cryptography issues, algorithms, and tools
m) programming skills
n) analytical ability

Appendix C: Roles and responsibilities

The following is a sample listing of the types of staffing, the range of positions, and the tasks for various positions that might be required for a CSIRT. Depending on the organizational structure of a team, the services it provides to its constituency, and the mission and goals of the team, there may be some subset of these roles that is identified to work on (or with) the CSIRT, or yet other roles identified that are not included here (e.g., legal representatives, policy developers, legal or criminal investigators, other liaison officers or management personnel).

Manager or team lead

1) provides strategic direction
2) enables and facilitates work of team members
3) supervises team
4) represents CSIRT to management and others
5) interviews and hires new team members

Assistant managers, supervisors, or group leaders

- supports strategic direction of assigned functional area
- supports the team lead as needed
- provides direction and mentoring to team members
- assigns tasks and duties
- participates in interviews with new team members

Hotline, help desk, or triage staff

- handle main CSIRT telephone(s) for incident or security reports
- provide initial assistance, depending on skills
- undertake initial data entry and the sorting and prioritizing of incoming information

Incident handlers

- undertake incident analysis, tracking, recording, and response
- coordinate the reactive and proactive guidance that will be provided to the constituency (develop material such as documentation, checklists, best practices, and guidelines)
- disseminate information
- interact with the CSIRT team, external experts, and others (such as sites, media, law enforcement, or legal personnel) as appropriate, by assignment from team lead or other management staff
- undertake technology-watch activities if assigned
- develop appropriate training materials (for CSIRT staff and/or the constituency)
- mentor new CSIRT staff as assigned
- monitor intrusion detection systems, if this service is part of the CSIRT activities
- perform penetration testing if this service is part of the CSIRT activities
- participate in interviews with new staff members as directed

Vulnerability handlers

- analyze, test, track and record vulnerability reports and vulnerability artifacts
- research or develop patches and fixes as part of the vulnerability response effort
- interact with the constituency, the CSIRT team, software application developers, external experts (CERT/CC, FedCIRC, vendors) and others (media, law enforcement, or legal personnel) as required
- disseminate information on vulnerabilities and corresponding fixes, patches, or workarounds
- undertake technology-watch activities if assigned
- mentor new CSIRT staff as assigned
- participate in interviews with new CSIRT staff

Technical writers

- assist and facilitate the CSIRT in the development of publications such as advisories, best practices, or technical tips

Web developers and maintainers

- maintain CSIRT web site
- create new content and corresponding designs for web site in conjunction with CSIRT staff
- administer web servers and application(s)
- maintain the web infrastructure, work closely with other system/network administrators

Trainers

- develop and deliver curriculum for teaching new incident handlers within CSIRT
- develop and deliver curriculum for constituency members
- provide security awareness training

Network or system administrators

- administer CSIRT equipment and peripheral devices
- maintain the infrastructure for CSIRT products; this includes secure servers, the data repository, secure email, and any other internal systems required by the CSIRT.

Support staff

- assist other technical and management staff as needed to perform administrative support services
- coordinate travel and conference arrangements as necessary

Platform specialists

- assist in analysis and response efforts by providing specific expertise in supported technologies or operating systems (e.g., UNIX, Windows, mainframes, applications, databases)
- may also perform incident handling, vulnerability handling or infrastructure tasks if needed

Appendix D: Resources

A variety of documents and other information are available through links on the CSIRT Development web pages at <http://www.cert.org/csirts/> and are included below. These describe current research projects underway in the global CSIRT community, as well as resources that can help with the development of CSIRTs:

1. *Creating a Computer Security Incident Response Team: A Process for Getting Started* < http://www.cert.org/csirts/Creating-A-CSIRT.html>
2. *The Handbook for Computer Security Incident Response Teams (CSIRTs),* 2nd Edition <http://www.cert.org/archive/pdf/csirt-handbook.pdf>
3. *State of the Practice of CSIRTs* <http://www.cert.org/archive/pdf/03tr001.pdf>
4. *Organizational Models for CSIRTs,* <http://www.cert.org/archive/pdf/03hb001.pdf>
5. *CSIRT Frequently Asked Questions* <http://www.cert.org/csirts/csirt_faq.html>
6. *CSIRT Services* <http://www.cert.org/csirts/services.html>
7. *Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?* <http://www.cert.org/csirts/csirt-staffing.html>
8. *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
9. *Practices for Outsourcing Managed Security Services* <http://www.cert.org/security-improvement/index.html#Contractors>
10. Best Practices Documents (RFC 3227, 2350) *Guidelines for Evidence Collection and Archiving,* <http://www.ietf.org/rfc/rfc3227.txt> *Expectations for Computer Security Incident Response* <http://www.ietf.org/rfc/rfc2350.txt>
11. Security Improvement Modules and practices <http://www.cert.org/security-improvement/index.html >
12. IETF Incident Handling Working Group (INCH WG) and Intrusion Detection Working Group (IDWG)
13. Automated Incident Reporting (AirCERT) <http://www.cert.org/kb/aircert/>
14. Clearing House for Incident Handling Tools (CHIHT) <http://chiht.dfn-cert.de/>
15. Common Advisory Interchange Format (CAIF) <http://cert.uni-stuttgart.de/projects/caif/>