Responding to a Customer's Security Incidents—Part 1: Establishing Teams and a Policy

Vijay Masurkar, Sun Services

Sun BluePrints™ OnLine—March 2003

http://www.sun.com/blueprints

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95045 U.S.A.
(650) 960-1300

Part No. 817-1795-10
Revision 06, 3/11/03
Edition: March 2003

Please
Recycle

Responding to a Customer's Security Incidents—Part 1: Establishing Teams and a Policy

There have been several large-scale worm attacks on the Internet since 1988 as well as highly visible and coordinated denial-of-service attacks in the last few years causing billions of dollars in damage. These attacks indicate that responding, if anything, to such incidents is increasingly more complex, and requires technical knowledge, communication, and coordination among the staff responding to an incident, along with an adherence to applicable standards.

A security incident response involves several aspects of preventive, detective, and recovery measures. A preventive measure primarily involves risk control that avoids or deters the occurrence of an undesirable event. Examples of preventive measures are passwords, keycards, badges, contingency plans, policies, firewalls, and encryption. A detective measure identifies the occurrence of an undesirable event. Examples of detective measures are visitor logs, audit trails, motion sensors, closed-circuit TV, and security reviews. Detective measures also provide a means for reporting the occurrence of events. A recovery measure is a risk control that will, in a traditional sense, include control policies, processes, or mechanisms that restore the integrity, availability, and confidentiality of information assets to their expected state. Examples of recovery measures are fault tolerance, backup, and disaster recovery plans.

Since the late eighties and early nineties, a substantial amount of information has been published on the topic of security incident response from the following organizations:

- National Institute of Standards and Technology (NIST), `http://www.nist.gov`
- Purdue University's Computer Incident Advisory Capability (CIAC), which is funded by the Department of Energy, `http://www.ciac.org/ciac`

- Carnegie Mellon University's Software Engineering Institute's Computer Emergency Response Team/Coordination Center (CERT/CC), which was initiated by the Defense Advanced Research Projects Agency (DARPA), `http://www.cert.org`
- Internet Engineering Task Force (IETF) in the form of RFCs

In 1990, NIST, in conjunction with CERT/CC, CIAC, NASA, and other agency response teams, organized a cooperative activity known as the Forum of Incident Response and Security Teams (FIRST), at: `http://www.first.org`

"Responding to a Customer's Security Incidents—Part 1: Establishing Teams and a Policy" is the first of a series of articles that discuss building teams, establishing a security incident response policy, and executing it. These articles are not intended to include all of the material from the above efforts. They are intended to capture the salient points of the security incident response process and to present them in the context of a business entity that serves its constituents (that is, its customers).

This document is intended to provide highlights and best practices information about computer security incident response, building teams to process security incidents, and developing important factors in establishing a security incident response policy framework. The primary audience consists of computer security managers, security policy developers, system administrators, and other related staff responsible for the creation or operation of a computer incident response team and/or a computer security incident response (CSIR) policy and service.

Computer Security Incident Response

Computer security incident response is the process and action an organization takes in response to a computer security incident. Any enterprise or organization that does business using computers, computer-based equipment, and/or data communications network should have a security incident response program to protect itself and its customers and partners before a security incident occurs.

Every security incident response program will contain unique elements that exist and make sense only for its organization. This article discusses only a common set of elements that can be followed. However, these elements must be treated only as a starting point for a more detailed analysis for a policy document.

In this article, we describe the essentials of establishing a security incident response policy for an organization within an enterprise. The organization could span all geographic zones, or it could be based in a specific geographic area. All organizations that ship computer-based equipment and/or software to their

customers need to define what a computer security incident is in relation to their own and/or customers' sites. General definitions for a computer security incident are:

- Any real, or suspected, adverse event in relation to the security of computer systems or networks
- Any act of violating an explicit or implied security policy

Examples of incidents include the following activities:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- Unauthorized use of a system for the processing or storage of data changes to system hardware, firmware, or software characteristics, without the owner's knowledge, instruction, or consent

Computer security incident activity can be defined as host or network activity that potentially threatens the security of computer or computer-based systems, networks, or sites with computing equipment. When a security incident is reported at an organization's customer site, the organization must process the incident responsibly.

Computer Security Incident Response Team

Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen, be successfully detected, or prevented every time. However, the speed with which an organization can recognize, analyze, deter, and respond to an incident will limit the damage and lower the cost of recovery.

A computer security incident response team (CSIRT) is a service organization that receives, reviews, and responds to computer security incident reports and activity and helps in recovery. Its services are usually performed for a defined constituency that could be a parent entity such as a corporation, governmental or educational organization, a region or country, a research network, or a paid client.

Why would some organizations want to form an incident response team? The following list contains a few of the advantages:

- Ability to effectively coordinate a response
- Ability to bring together a team of experts to analyze and solve complex incident issues
- Ability to improve overall efficiency of an organization's response processes

- Ability to work proactively
- Ability to create a liaison to deal with institutional barriers, because generally the teams are able to exert more authority than an individual

While the benefits of CSIRTs are obvious, the task of forming and operating a CSIRT is fraught with pitfalls that can result in the demise of a team. Thus, it must be emphasized that to ensure an infrastructure of a competent and respected CSIRT, supporting information and guidance are extremely important. Successful metrics must be established to indicate the degree of success in the actions taken to deal with incidents. A number of possible metrics for incident response exist:

- How many incidents has the response team dealt with in a given time period?
- How many incidents resulted in an estimated financial loss that is below a certain value?
- What were the average time and resources needed to resolve each incident, plotted against the apparent complexity of an incident?

Self-evaluation measures, such as questionnaires, can be used; however, none of the metrics, or even a combination of them, can be adequate to measure the success of a CSIRT. A CSIRT should view such metrics as a start, and ultimately, develop its own metrics that satisfy and suit the organization and the constituency it serves.

Is a team really necessary? It is not always advantageous to create a CSIRT. An alternative is to use individuals who are not part of the incident response team, but who are available (usually based on prior agreements, such as service-level agreements, between organizations) when incidents occur. There are some possible advantages of adopting such an alternative. Smaller organizations generally do not need a team; the overhead costs can outweigh the advantages. In addition, due to the lack of resources, forming and deploying a team could become a difficult goal to achieve. This is because personnel with computer security expertise are hard to find. The following is a list of recommended steps to form a team in an organization. These steps do not have to be followed in the sequence shown:

1. Obtain management support and buy-in for human resources and costs.

   This should involve informing executives such as the chief information officer or the chief security officer.

2. Determine the CSIRT strategic plan for the team's goals and operations, and gather pertinent information to help in understanding past and current issues.

3. Design the CSIRT vision by defining the charter and goals and identifying the constituencies.

4. Communicate the vision and operational plan to management, constituencies, and others who need to know and understand the teams' operations.

5. Start the CSIRT implementation by hiring the appropriate staff and acquiring the needed equipment, as well as defining the required policies. (See “Computer Security Incident Response Policy” on page 17.)

6. Announce the operational CSIRT to the constituencies and the parent organization that provided the resources.

7. Evaluate the CSIRT effectiveness periodically with the appropriate metrics. The metrics could need to be fine tuned.

There is another angle to pursue and evaluate when an organization is initially considering to form a team to respond to security incidents. Should it have its own incident response team, or should it outsource the effort to provide incident response support? One of the many advantages of contracting with a commercial CSIRT is that the overall cost of dealing with incidents is likely to be lower because incident response personnel (contractors or consultants) need to deal only with incidents that occur. Unless there is a plethora of incidents, there is no need to keep a full-time staff waiting for incidents to occur. This can be a viable alternative not only for small companies but even for large ones when there is no trained staff available or when recruiting for a proposed CSIRT.

A CSIRT can be a formal or an informal team. A formal team performs incident response work as its major job function. In this article, we do not define the membership of a formal CSIRT. An informal team is called together to respond to an incident when the need arises. In this article, the informal team is referred to as a virtual CSIRT (or VCSIRT), and its membership is defined in “VCSIRT Team Members on page 8. Although initiated by an organization's security team (referred to as the worldwide security team) to resolve a particular incident or a set of related incidents, a VCSIRT can span several organizations within an enterprise, as shown in the following figure.

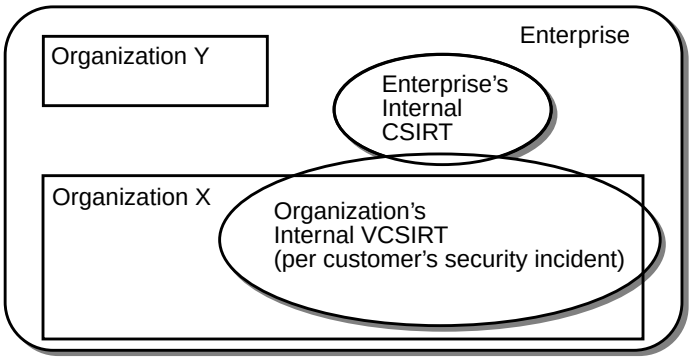

FIGURE 1 CSIRT and VCSIRT Within an Enterprise

The following list contains the typical functions of a CSIRT:

- Announcements regarding current or potential threats
- Vulnerability announcements and responses
- Artifact analysis and response (*artifact* typically applies to potentially malicious software left by an intruder on the compromised system or network)
- Education
- Incident tracing
- Intrusion detection
- Security consulting (serving as a clearinghouse for security information)
- Risk analysis
- Technology watch
- Security process development
- Collaboration
- Cooperation with other internal or external related entities

These functions are usually performed in varying degrees by an enterprise's CSIRT. However, collaboration and cooperation activities are significant with any kind of CSIRT. An organization's VCSIRT usually focuses on the mandatory services pertaining to a particular security incident response. It is expected that an enterprise CSIRT and one or more VCSIRTs will communicate with each other and that the information flow between them will be well-defined.

VCSIRT Team Members

This section includes descriptions of key individuals who can form the wider VCSIRT community.

Note – Depending on the geographic area, the size and type of the organization and the enterprise membership can differ; however, the underlying representation requirements are important. A VCSIRT team could consist of any combination of the individuals listed below, or others, but at least one person with security responsibilities is required to be in the team.

- Enterprise service engineer

  This person is responsible for covering the customer site's installation, maintenance, and/or support.

- Technical support person

  This person is typically in the enterprise's customer service center and gets involved when contacted by an enterprise customer, a partner, or an enterprise field engineer.

- Enterprise's security coordinator

  This person coordinates security fixes to the enterprise's products and services by planning for and acquiring internal enterprise resources. Usually, it is also the responsibility of this individual to monitor security vulnerabilities reported to the industry or to the enterprise, set priorities for the issues rising from the vulnerabilities, and take appropriate steps to protect the enterprise's, customer's, and business partner's interests by coordinating necessary actions within the enterprise. If an incident is reported by customers using the `security@`*company*`.com` alias, this person assists in the coordination of the response.

- Geo-based customer account manager

  This person is responsible for the customer account for the site in question.

- Enterprise's CSIRT assigned contact

  This person gets involved in cases in which the enterprise's equipment (such as their WAN) is affected.

- Organization's geo-based security officer

  This person is responsible for the security of all of the organization's customer installations in that geographic area. Every geographic area is expected to have a security officer.

- Organization's worldwide security manager

  This person is responsible for the overall security policy and manages all of the geo-based security officers for the organization, in addition to other staff members, such as security administrators and policy developers.

- Personnel relations (PR) officer

  This person could be needed depending on the situation (for example, to avoid media coverage). Usually, the PR officer is a corporate-level PR employee in the enterprise.

- Enterprise's legal counsel

  This person is required when prosecutions, lawsuits, or possible regulatory violations are involved, but can also provide guidance when sensitive verbal or written communications with external parties are prepared and delivered.

User Community

Discretion should be used when notifying users. Users can be of the following types:

- Enterprise’s employees (that is, customer service engineers, organizational administrators, and other enterprise employees)
- Enterprise’s business partners
- Enterprise’s customers

Because users could also be customers, an extremely careful analysis of information and wording of the notice is necessary.

Public Relations

The enterprise's PR office must be consulted when any incident needs to be reported externally through the organization's worldwide security manager. However, the organization's geo-based customer account manager or the geo-based security officer, in the account manager's absence, should maintain the focus over the incident. In addition, the geo-based security officer should closely monitor the incident and the geo-based customer account manager's actions to maintain the necessary rapport with the site in question.

Involvement of the Organization's Teams

FIGURE 2 on page 11 shows the involvement of the organization’s teams for one or more incidents. For a particular geographic area, there is a one-to-one relationship between the customer, the geo-based VCSIRT, and the geo-based security officer. However, a single geo-based security officer could be involved in overseeing more than one incident and, hence, more than one VCSIRT and customer.

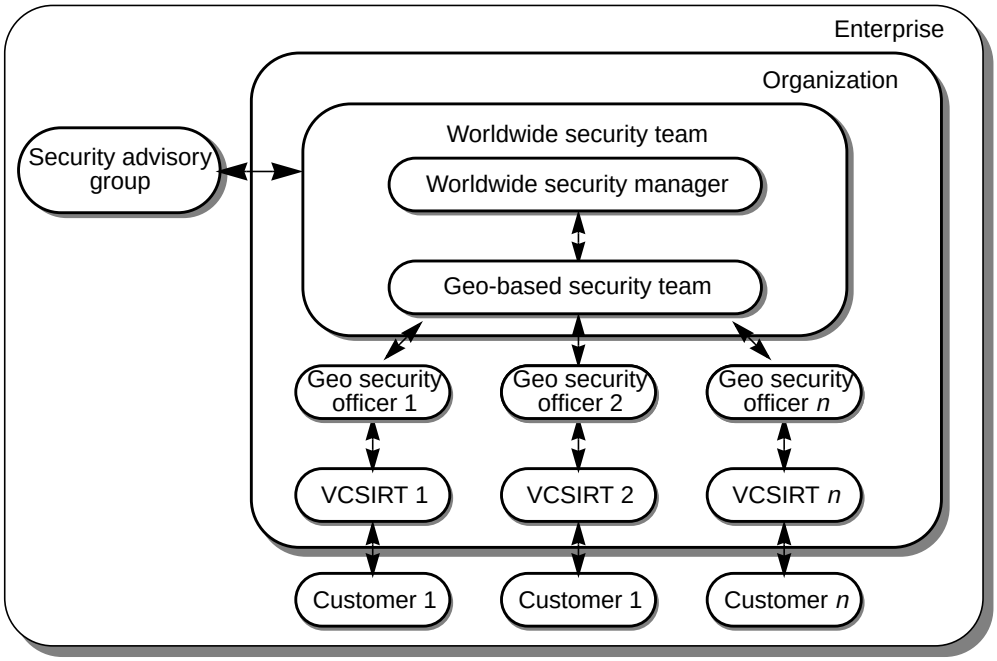

FIGURE 2 Organization's Security Teams

Worldwide Security Team

This team consists of the worldwide security manager of the organization and the geo-based security officers, along with other security-related staff such as policy developers and security engineers. The scope of their work covers all of the organization's customers, partners, and vendors.

Geo-Based Security Team

This team includes the geo-based security officer and all of the organization's customer account managers within that geographic area. Local security experts of the organization could also be part of this team. The scope of this team could be limited to a part of a country or one or more countries within a geographic area. Each geo-based customer account manager has security monitoring jurisdiction over his or her region, along with the geo-based security officer.

Virtual Computer Security Incident Response Team

The virtual computer security incident response team (VCSIRT) is formed by the geo-based security officer to make quick progress on a specific security incident. This team should consist of at least the security officer, the geo-based customer account manager of the region where the incident took place, and the organization's or enterprise's technical persons (for example, field engineers, technical support engineers, or computer forensics experts) involved directly in reporting, following, or mitigating the impact of and/or recovery from an incident.

Security Advisory Group

The security advisory group (SAG) is an enterprise-wide entity and is independent of any specific organization within an enterprise. Its primary functions include advising on tactical and long-term strategies, reviewing the organization's policies, and providing recommendations. SAGs can be initiated and formed by organizations for indefinite periods of times, or for long as they are deemed necessary. SAGs use resources from the entire enterprise. By the advisory nature of its function, a SAG should include highly experienced security experts, ideally covering different aspects of security.

Security Team Interactions

FIGURE 3 on page 13 shows the scope of operations and interactions among an enterprise's security teams that are involved in its customer's security incident response. This is just an example for best practice. The communications framework differs according to the size and type of an enterprise. There are two organizations shown within an enterprise. Each has its own SAG and worldwide security team for assisting customers on security and incident response with respect to their products, services, and operations at the customer sites. The SAG can be outside of the organization, with members from the organization's worldwide security team. A VCSIRT can be formed per incident by an organization, depending on the need, with members from inside or outside the organization (as shown with its coverage outside of the organization). The corporate security team is usually involved with all organizations, as the need arises, in resolving major security issues and communicating with the SAGs. However, an organization's worldwide security team can also choose to communicate with the corporate security team, which for a medium to large enterprise, is usually a central team in the enterprise. The internal CSIRT of an enterprise is a resource to the VCSIRTs and is formed by organizations. They can become a focal point for incident processing, particularly when the enterprise is at risk.

In a relatively large enterprise, all of these teams could co-exist in varying combinations; while, in a small company with minimal resources, only a single security team could handle every incident. In such a case, it is recommended that functional responsibilities be assigned to one or more members who are represented in the diagram by the teams' major functions.

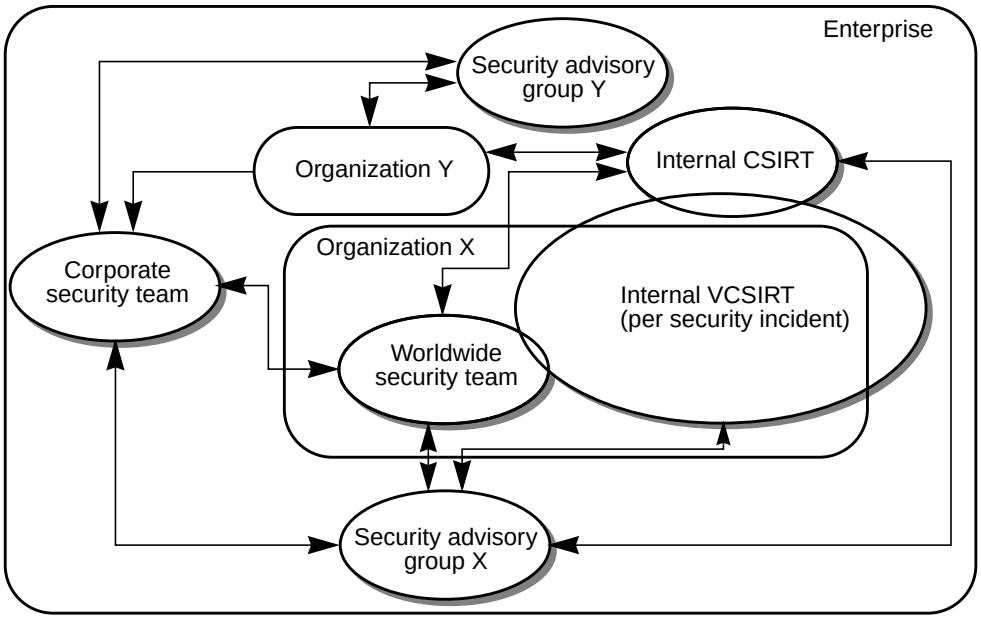

FIGURE 3 An Example of the Enterprise and Organizational Security Teams

By exchanging information, cooperating teams usually benefit, and in turn, their customer constituencies benefit as well. Information is exchanged not only between the teams in an enterprise, but also between an enterprise's internal CSIRT and external CSIRT. Exchanging information across country borders requires special attention to the laws of the countries involved. Also, it is more appropriate to service an incident local to its occurrence where local needs, language, time zone, and other requirements can be met. For example, there have been instances in which a CSIRT in a European country has contacted CERT in the U.S.A., without realizing that a national-level CSIRT exists. In this case, CERT diligently responded to the request for immediate assistance, then referred the CSIRT to the appropriate national-level CSIRT for further help.

As summarized in the following table, formal agreements between teams clarify solutions to issues regarding the use and exchange of information.

Information Issue	Description
Confidentiality and/or secrecy	As the information could be valuable to other parties, its confidentiality and/or secrecy must be maintained. This is true for the transfer, storage, and actual usage of the information.
Appropriate use	While the information belongs to one team, it must be clear to other teams that they must adhere to guidelines of *appropriate use*, as outlined by the originating team. In this context, it is assumed that appropriate use includes information creation and destruction, and classification and declassification.
Disclosure	As the information could be distributed to the public in the future, disclosure restrictions must be stated.
Proper acknowledgements	Because the information was collected, analyzed, and made available by other teams, the team using it should consider a fair and proper acknowledgement of the source.

Definition and Relationships of Constituency

A constituency is the specific community that a CSIRT is established to serve. It is also the most important party among a wide range of parties the CSIRT needs to interact with during the course of its operation. Most commonly, CSIRTs have bounded constituencies that tend to reflect the CSIRT funding. Human resources, costs (which differ depending on the size, type, and needs of a constituency), and risks must be taken into account. Defining a constituency is not a trivial task, as it first seems. Constituencies of customers or customer sites can be defined by a number of constraints, such as:

- Geographical boundaries
- Network provider
- Organizational dependencies

The nature of the relationship between a CSIRT, or CSIRT-related teams, and its constituency directly impacts the nature of the services that the CSIRT offers. In general, for accomplishing best practices in cooperation and collaboration, there are four categories of authority for the teams that must be considered: full, shared, none, and indirect, as summarized in the following table.

Level of Authority	Team Examples	Constituency Relationship
Full	VCSIRT, plus worldwide security team or geo-based security team	The members of these teams have the authority to undertake any necessary actions or decisions on behalf of their constituency.
Shared	VCSIRT	The members provide direct support to their constituents (per incident basis) and share in the decision making process with the worldwide security team. In other words, they can influence constituency decisions, but they are unable to dictate them.
None	SAG	The members of the SAG have no authority over their constituency and can act only in the role of an advocate or in an advisory capacity.
Indirect	Enterprise's CSIRT	The team members of the enterprise's internal CSIRT can exert pressure on its constituency (which is the enterprise itself, including all of the organizations and their VCSIRTs) to enforce certain rules when dealing with customer issues that may affect, for example, the enterprise's WAN.

Functions of the Security Incident Response Service

For each service, among a range of services provided, a CSIRT must provide its constituency with service descriptions (or formal Service Level Agreements) in as much detail as possible. These descriptions are helpful to the team when defining, implementing, and operating the service. In particular, the descriptions should include an explanation of the items, such as:

- Objective of the service
- Scope and depth
- Functions
- Availability (to whom, when, and how)
- Quality assurance parameters (to set limitations on constituency expectations)

- Interactions and information disclosure
- Interfaces with other services
- Priorities of the services, with respect to other services, and of functions, with respect to other functions in a service

The security incident response service, reflected in the establishment of a Security Incident Response Policy and provided by a security team such as an organization's worldwide security team, usually consists of the following four functions:

- Triage
- Incident management
- Announcement
- Feedback and proactive measures

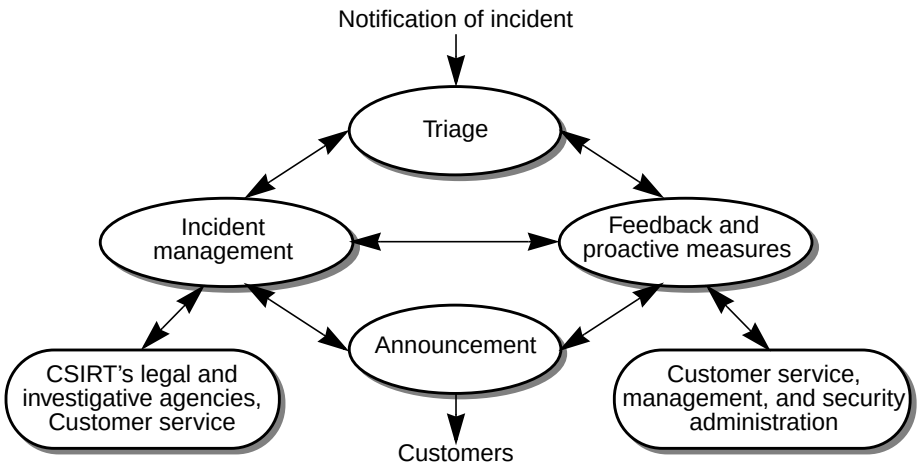

FIGURE 4 Organization's Worldwide Security Team's SIR Service Functions

In the context of this article, the triage function provides a single-point-of-contact for accepting, collecting, sorting, and passing on incoming information from the affected customers for the SIR service. The incident management function provides support and guidance related to suspected or confirmed computer security incidents at customer sites. This function primarily includes the notification, evaluation, containment, and eradication of an incident. In addition, legal and investigative resources could be involved, as appropriate, and post-incident procedures could be developed. The feedback and proactive measures function consists of feedback on issues not related to specific incidents, but it can involve answering frequently asked questions relating to SIR, and developing and maintaining proactive measures for reducing the risks of future harm. Lastly, the announcement function generates

information tailored for the specific customer constituency. (Part of the incident management function and the feedback and proactive measures function are described in a follow-up article.)

Computer Security Incident Response Policy

Every organization has, or claims to have, a security policy that embraces all security aspects, ranging from locks on doors to backups, passwords, firewalls, encryption, security incidents, and more. This article discusses only those aspects of best practices that apply to the security incidents at an organization's customer sites.

The computer security incident response policy (CSIRP) should be an integral part of the organization's overall security policy. CSIRP primarily addresses the responsibilities of the CSIRT and VCSIRT in the organization's infrastructure. It should also address the following items in regard to a security incident:

- Preparing and planning for handling an incident
- Setting of clear priorities
- Notifying of an incident
- Identifying an incident
- Handling of an incident
- Executing of a response to an incident
- Determining of the implications of past incidents
- Recording and preserving the analysis of past incidents and learned lessons

The primary benefits of defining and maintaining an SIRP are:

- Recovery from loss or potential loss
- Resource optimization within the organization, its customer, partners, or vendors, including suppliers
- Protection of classified, sensitive, or proprietary information that belongs to the organization, its customer, partners, or vendors, including suppliers
- Management of public relations under a security crisis that could affect the organization, its parent enterprise, its customer, partners, or vendors, including suppliers
- Prevention of legal actions against the organization and its parent enterprise

While developing the policy, it is important to keep in perspective the information security principles defined by the International Information Security Foundation as best practices (for more information, see the GASSP entry in “References” on page page 23).

Scope of the Policy

Developing and defining the scope of the policy requires careful analysis with risks and responsibilities taken into account. This section provides a specific example of how the scope can be defined for an organization's CSIRP. It is important to note that the rest of this article, and the next article, addresses the essential policy aspects within this scope.

The policy typically applies to the use of enterprise-owned, hosted, rented, or leased computers or computer-based equipment, network equipment, operating systems, and application software, which compose the organization's processing environment. The policy also applies to the organization's or its parent enterprise’s entire family of products and services at the customer site. Further, the policy applies to the organization’s, its vendors’, and partner’s facilities and systems in customer’s facilities that are owned or managed by the enterprise, its vendors, suppliers, or partners. The following entities and users should be covered by this policy:

- Full or part-time employees and contractors within the enterprise who use or access data, systems, or networks
- Vendors who are authorized to use enterprise-owned equipment, systems, applications, or facilities
- Authorized persons, entities, or customers who have access to the organization's or enterprise’s services, facilities, systems, or applications
- External partners that must support audit mechanisms, in compliance with the organization's or third-party agreements and legal, regulatory, or fiduciary mandates

Security Incident Response Policy Goals

The goals of the SIRP for the organization are as follows:

- Research how an incident happened

  This is to learn how the intrusion happened, what components were affected, and what damage, if any, was caused.

- Investigate the root cause

  To understand the root cause, involvement by more than one organization or business enterprise could be needed. Understanding the root cause could prevent future compromises.

- Assure integrity of critical systems

  The critical systems for the enterprise are the organization's computing systems and all of the network equipment associated with the enterprise's WAN, as well as customer systems running hardware and software supported by an enterprise's organization.

- Maintain and restore data

  Data availability is essential, so if data is stolen or corrupted intentionally, it needs to be restored as quickly as possible, while preserving any data that may be considered evidence.

- Maintain and restore services

  The services of the organization depend on the various computer-based or computer systems and networking components. These need to be brought back online if they are shut down or not completely functional.

- Take corrective action

  Taking corrective action ensures that the potential for recurrence is eliminated.

- Improve the policy and processes

  To avoid future incidents, the policy and processes must be continually improved with analysis and learned lessons from past incidents.

- Avoid negative publicity

  The appropriate enterprise resources (for example, the enterprise's legal or public relations department) should be consulted as necessary.

Breach of Policy and Enforcement

A breach of the SIRP could affect an organization's ability to prepare for and to track security compromises, penetrations, and attacks. Any person who causes the failure, disruption, or destruction of the procedures, guidelines, data, or evidence should be subject to disciplinary action at the discretion of the organization's and the enterprise’s management.

Local laws and regulations differ from country to country. Therefore, CSIRTs need to be aware of the constantly changing legal framework of the environment in which they operate, and they must adapt accordingly. Before enforcement, a CSIRT should ensure that it limits its legal exposure by clearly declaring within its charter what its

purpose, goals, and scope, are and what it is and is not purporting to do. Appropriate legal advisors need to review the charter and all of the procedures in use by the incident response teams.

Notification of a Security Incident

This section contains descriptions about who can report an incident, how an incident can be reported, how it should be communicated, and the points of contact within an organization.

Who Can Report an Incident

A security incident can be reported by anyone, yet it is typically reported by any of the persons listed below, who are involved in the installation, monitoring, support, or management of the organization's products or services at the customer sites (the following list is not all-inclusive):

- Geographically-based (geo-based) customer account managers
- Computer system administrators
- Security administrators
- Security managers
- Technical support engineers or field engineers and related staff physically located outside of the organization's main sites, at customer sites, or at customer service centers
- Enterprise’s customers, partners, or vendors
- Enterprise's employees and / or contractors

Communication Entry Points

Reporting an incident can happen in multiple ways, as indicated below, but are not limited to the following:

- Phone calls, e-mail messages, or faxes of an incident description to the organization's security personnel
- Reports to the enterprise's CSIRT
- Reports to the organization's security web site, following the procedures and conditions listed on the site (for example, for high urgency)

- `security@`*company*`.com` alias of the enterprise
- Organization’s or enterprise’s customer service centers

It is important to note that the organization's geo-based customer account manager is jointly responsible for the organization's security site, along with the organization's security officer for that geographic area. Together, they form the VSCIRT team that follows up on the incident.

Communication

The organization's security officer and / or worldwide security manager should communicate through a well-known email alias with all of the parties that need to be aware of a compromise and its implications. Established secure communication mechanisms should be deployed to accomplish this.

Executing information dissemination procedures include, but are not limited to, contacting users affected by an intrusion, security personnel, law enforcement agencies, vendors, and other security incident response teams, internal or external to the enterprise.

What a security incident covers must be stated in a written format and provided on an internal public web site. Priority definitions must be provided for all types of reported emergencies.

Explicit Nature of Communication

All notification information must be clear, concise, and fully qualified using a standard notification form, specified by the organization's security advisory group. Bear in mind that choice of language and cultural differences are important factors for communication.

Factual Information—Written and Spoken

Written information must be factual and sent though fax or email in a secure manner. When information is transmitted verbally, it should describe the incident clearly without generating undue alarm or confusion.

Technical and Non-Technical Explanation

Depending on the parties involved in processing an incident, it could be necessary to clearly explain the security incident in a technical manner, as well as in a non-technical manner.

Points of Contacts

The primary, incident-related points of contact (POCs) are the organization's geo-based customer account manager, who is responsible for the installation of products and services at the customer site, and the geo-based security officer. Alternatively, or on a temporary basis, the POC could be an employee from the enterprise's CSIRT, such as a security administrator, or any enterprise employee on a *hotline* (for example, a technical support engineer). This POC must be the focal point for collecting and disseminating information until other arrangements are made by the geo-based security officer.

External Contacts

The enterprise's corporate security must maintain contacts with the local security manager, the organization’s worldwide security managers, and the country’s federal law enforcement agencies, as necessary, during the course of an incident.

The enterprise's security coordinators, who could be members of the corporate security team or an independent organization, must maintain a contact list, including the following:

- CERT (`http://www.cert.org`)
- FIRST (`http://www.first.org`)
- CSIRTs outside of the enterprise
- Internet service providers
- Customer (constituency) site security contacts
- Other sites that are external to the constituency
- Participating vendors and partners
- Security experts
- Media contacts

About the Author

Vijay Masurkar is a Senior Consulting Engineer and Services Architect for Network and Security within Sun Support Services. His current research interests are best practices for network and security and enterprise and Internet-level reliable and secure architectures for applications and middleware. Vijay has been in the computer network and security industry for twenty-eight years. He has led research and development projects, consulting, and support for VAX/VMS, Wang VS, the Solaris OE, and TCP/IP-based network and security technologies, services, software products, and development tools. He represents Sun in several industry forums and is often invited to teach at Sun and in the industry. Vijay holds a B.S. degree in Electrical Engineering, an M.S. degree in Computer Systems Engineering, and an M.B.A.

Acknowledgements

The author would like to recognize the following individuals for their contributions:

- Senior personnel from Sun Services and Sun Corporate and IT Security for reviewing this article and providing helpful comments, in particular, Joel Weise, Martin England, Glenn Brunette, and Scott Elam
- Sun BluePrints™ personnel who contributed in editing and revising this article

References

The following references were used to write this article:

- CERT, Software Engineering Institute, “CSIRT FAQ,” Carnegie Mellon University, 2002, `http://www.cert.org/csirts/csirt_faq.html`
- CERT, Software Engineering Institute, *Handbook for Computer Incident Response Teams*, Carnegie Mellon University, December 1998
- CSI and FBI, “2002 CSI/FBI Computer Crime and Security Survey,” January 2003, and similar reports from earlier years
- Fraser, B., ed. *Site Security Handbook*, RFC 2196, Internet Engineering Task Force, September 1997

- International Information Security Foundation, “Generally Accepted System Security Principles,” January 2001, http://web.mit.edu/securitywww/GASSP/GASSP.doc
- Smith, Danny, “Forming an Incident Response Team,” FIRST Conference, July 1994, Australian Computer Emergency Response Team, http://www.auscert.org.au/
- Weise, Joel, and Charles R. Martin, “Developing a Security Policy,” Sun BluePrints OnLine, December 2001, http://www.sun.com/blueprints/

Ordering Sun Documents

The SunDocs℠ program provides more than 250 manuals from Sun Microsystems, Inc. If you live in the United States, Canada, Europe, or Japan, you can purchase documentation sets or individual manuals through this program.

Accessing Sun Documentation Online

The docs.sun.com web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is http://docs.sun.com/

To reference Sun BluePrints OnLine articles, visit the Sun BluePrints OnLine Web site at: http://www.sun.com/blueprints/online.html