



# Responding to a Customer's Security Incidents—Part 2: Executing a Policy

*Vijay Masurkar, Sun Services*

*Sun BluePrints™ OnLine—April 2003*



<http://www.sun.com/blueprints>

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

Part No. 817-1796-10  
Revision 13, 4/11/03  
Edition: April 2003

Copyright 2003 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95045 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Sun BluePrints, Solaris Security Toolkit, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the US and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

---

Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95045 Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. a les droits de propriété intellectuelle relatants à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains énumérés à <http://www.sun.com/patents> et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les Etats-Unis et dans les autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque enregistrée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company Ltd.

Sun, Sun Microsystems, le logo Sun, Sun BluePrints, Solaris Security Toolkit, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.



Please  
Recycle



Adobe PostScript

# Responding to a Customer's Security Incidents—Part 2: Executing a Policy

---

There have been several large-scale worm attacks on the Internet since 1988 and highly visible and coordinated denial-of-service attacks in the last few years causing billions of dollars in damage. These attacks indicate that responding 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 and policies.

A security incident response involves several aspects of preventive, detective, and recovery measures. A preventive measure primarily involves risk control that mitigates the effects 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:

- Australian Computer Emergency Response Team (AusCERT),  
<http://www.uscert.org.au/>
- Brazil's Centro de Atendimento a Incidentes de Segurança (CAIS),  
[http://www.rnp.br/lang/cais\\_en/](http://www.rnp.br/lang/cais_en/)

- 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>
- European Institute for Computer Antivirus Research, <http://www.eicar.org/>
- German Computer Emergency Response Team (DFN-CERT), <http://www.cert.dfn.de/>
- Internet Engineering Task Force (IETF) in the form of RFCs, <http://www.ietf.org/rfc.html>
- Purdue University's Computer Incident Advisory Capability (CIAC), which is funded by the Department of Energy, <http://www.ciac.org/ciac>
- SysAdmin, Audit, Network, and Security, <http://www.sans.org>
- U.S.'s National Institute of Standards and Technology (NIST), <http://www.nist.gov>

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>

This coalition brings together a variety of computer incident response teams from governments, commercial organizations, and academic organizations. FIRST fosters cooperation and coordination in incident prevention, prompts rapid reaction to incidents, and promotes information sharing and learning among the members of its community.

“Responding to a Customer’s Security Incidents—Part 2: Executing a Policy” is the second of a series of articles that discuss a security incident response policy and execution. 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).

The first article, “Responding to a Customer’s Security Incidents—Part 1: Establishing Teams and a Policy,” contains definitions of security incidents, security incident response, teams that typically are involved in an incident response, the pros and cons of the teams, and the scope and goals of the security incident response policy. In addition, it describes policy essentials for the notification aspect of a security incident.

This second article describes the best practices and execution of key policy features of responding to a customer’s incident within the policy scope described in the first article. These features mainly include evaluation, containment, and eradication of and recovery from a security incident. Subsequent articles will focus on incident follow-up, with a special emphasis on forensics, risk analysis, disaster recovery, and

government and legal recourses, as well as proactive teamwork. 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 security incident response policy and service.

---

## Security Incident Response

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 for security incident response. 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 executing 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.

---

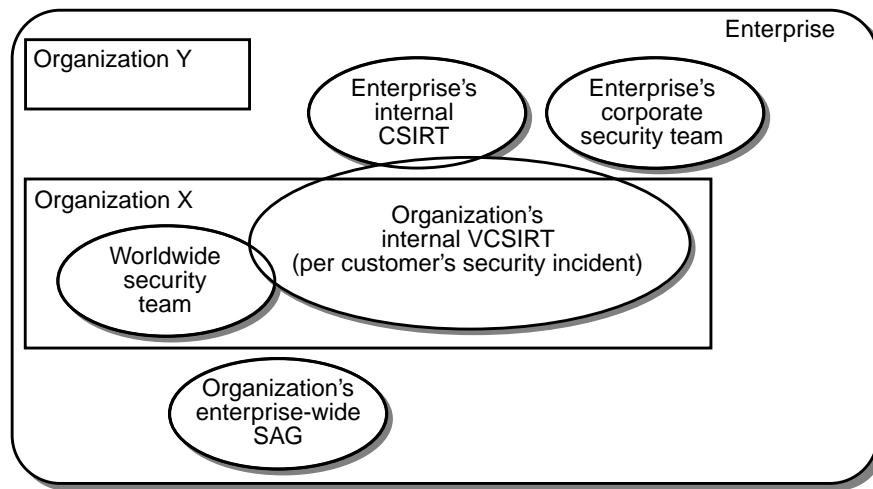
## Computer Security Incident Response Teams

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

A CSIRT can be a formal or an informal team. A formal team performs incident response work as its major job function. An informal team is called together by the organization's worldwide security team (as defined in the first article) to respond to an incident when the need arises. The informal team is referred to as a virtual CSIRT (VCSIRT), as defined in the previous article, along with its membership.

Although initiated by an organization's security team to resolve a particular incident or set of related incidents, a VCSIRT can span several organizations within an enterprise, as shown in the following figure and described in the first article. From the policy execution point of view, there are pros and cons to having VCSIRTs. For

instance, virtual teams can be cost-effective from the operational point of view, as such teams do not have to wait for incidents that might not occur on a frequent basis. However, VCSIRTs have disadvantages from the policy execution perspective. Trained experts cannot be summoned at a moment's notice because they are usually in high demand. Secondly, on-the-fly teams do not bond as well as those that are gathered with the purpose of maintaining longer associations.



**FIGURE 1** Enterprise and Organization Security Teams

The figure shows the corporate security team that sets security policies, processes, and procedures for the entire enterprise and monitors them for compliance. An enterprise should have an internal CSIRT that responds to the enterprise's internal incidents and sets related policies, processes, and procedures. The security advisory group (SAG) is an entity that can have enterprise-wide representation and is independent of any specific organization within an enterprise. Its primary functions include advising on tactical and long-term strategies, reviewing policies, and providing recommendations. SAGs can be initiated and formed by organizations for indefinite periods of times or as long as they are deemed necessary. SAGs use resources from the entire enterprise.

---

**Note** – The above structure of teams might not be possible in a small company; in which case, individuals might represent the functions of the teams, and there might be just one security team in the company that sets and monitors corporate security policies and handles all incidents. Also, in small, medium, and large enterprises, variations in the form of such groups can occur based on business needs. The essence we want to convey is that the functions performed need to be represented in the organizational infrastructure.

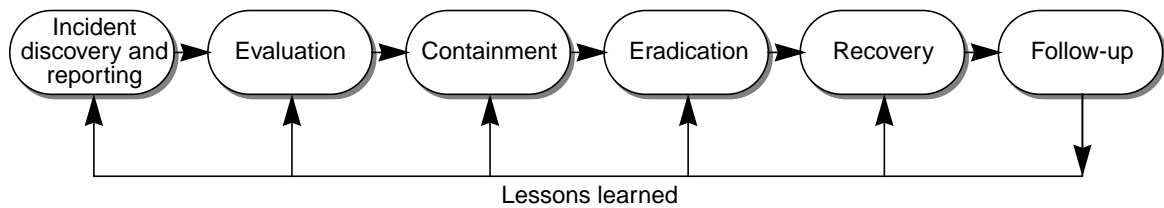
---

---

## Preparing for Incident Response

An organization and its constituents must be prepared to respond to an incident, just as it must be prepared to react to any other kind of emergency (for example, a fire). Also, ideally, constituents (that is, an organization's customers in the context of this article) and CSIRTs are expected to prepare for incidents before any incident actually happens. Although, in most cases, preparations happen in stages to reach a completed state. (Proactive teamwork in this area is addressed in detail in the last article in this series.)

The incident response process is summarized in the following diagram:



**FIGURE 2** Computer Security Incident Response Process Diagram

As shown in Figure 2, there are six primary phases that the incident response policy must cover:

- Discovery and reporting
- Evaluation
- Containment
- Eradication
- Recovery
- Follow-up

All six phases are equally important to prepare for and to ensure that a security incident is quickly resolved with a minimum impact to the business operation. The follow-up phase includes a postmortem session that is extremely important for the VCSIRT and the worldwide security team to review areas that are overlooked during the process. A shortfall at any phase might impact the process in the next phase and might ultimately affect the entire process. Every incident is unique, and the experience gained from handling one incident can provide lessons that are helpful in different phases, as depicted in the feedback loop in the diagram.

Complexity of the incidents and their implications in terms of losses to businesses have made it an absolute necessity to prepare. The primary categories of tasks include:

- Obtaining personnel who are skilled in security for incident servicing organizations to deal with incident issues as they occur
- Setting up defense-in-depth within the infrastructures (defined in the next section) at the constituent site and at the VCSIRTs parent organization's site for communication between them
- Establishing an infrastructure in the customer's enterprise to support incident response process and to mitigate risks that have adverse effects on the business
- Creating the servicing enterprise organization's infrastructure processes and procedures to deal with incidents effectively

In the early stages of the formation of the organization's worldwide security team, there will be ad hoc approaches to incident response, but as the organization becomes more established and mature, policies, procedures, and standards must be developed. This topic will be discussed in detail in a future article on proactive teamwork.

## Designing and Deploying Defense-in-Depth

Defense-in-depth is widely misunderstood. It is not just about technology, security experts, or policies and processes. It is multidimensional with time-honored improvements included, as discussed below. Having wide-open systems that are completely vulnerable to attack with a strong incident response policy and deployment is simply unreasonable. On the other hand, having strong defenses without having strong matching strength in response capability is naive. Thus, it is important to achieve a balance between these two extremes. The goal should be to allocate appropriate resources to achieve a baseline of security in systems, networks, devices, applications, middleware, operating systems, and databases. Therefore, incidents in which the risk is assessed to be very high are not likely to become commonplace.

## People, Technology, and Continuous Process Reinforcement

First, the challenge here is to use security-trained personnel and multiple, independent, different, and mutually-reinforcing security technologies to safeguard the constituent's enterprise, the servicing organization's infrastructure, and their communications. The concept of defence-in-depth can be applied to an N-Tier architecture, which involves the grouping of systems that have similar services, security risks, and exposure. The premise is that no layer, device, or choke point should be a single-point-of-failure for the organization's customer site. By isolating

the servers and services, an intruder who attempts to gain access to the site will have several layers of security to overcome before gaining access to the customer's sensitive information systems.

Second, irrespective of how tightly the security was designed and deployed, it is important to understand that security is an ongoing process. The process needs to be reviewed and upgraded periodically as weaknesses are discovered.

## Risk Consideration

Secure, defense-in-depth design, with risk analysis in mind, impacts all of the components of an enterprise (for example, servers, hubs, switches, routers, firewalls, LANs, WANs, and wireless LANs—WLANs). In a future article in this series, risk analysis, with alternative ways to assess risk, will be discussed. However, in this section, we present two basic tenets of risk analysis that can guide personnel and organizations when designing and making changes to their computer-based infrastructures, to which the above components belong:

- Principle of least privilege

Anything that is not expressly permitted is denied. This is well known in the security industry. For instance, this tenet is applied to firewall rules to allow only the absolutely necessary services to go across the firewall. It also applies to physical security (for example, in the distribution of keys and other access devices). Does Joe, who is a member of a VCSIRT, have a legitimate business need to have a key to the worldwide security team's lab? He certainly does. Does he have a need to access the chief security officer's office? Definitely not.

- Compartmentalization of information

This tenet is actually a subset of the principle of least privilege. Information should be accessible and distributed on a *need-to-know* basis. There is a reason for a member of the VCSIRT or the enterprise's CSIRT to access the engineering information for an enterprise's security product from the parent of the organization to which the worldwide security team belongs; however, the team member does not have a reason to access human resource files for the worldwide security team members.

---

## Management of Security by Teams

Because security teams typically have high profiles, attacks on their systems and networks can be expected. Intruders might retrieve critical information, such as past mission-critical intrusions; hence, the team's operational information and associated infrastructure are attractive targets. For example, a smart attacker could alter the parameters of an internal firewall that the organization's VCSIRT is using and allow

certain destructive services to enter into the team's internal network. That is why, in addition to having their own security policies, security teams such as incident response teams must place great emphasis on guarding their own security by considering the following factors in the execution of their policies and procedures.

- Confidentiality

Teams should get what is allowed and what they are supposed to get, nothing more. There is a lot of information gathering that occurs during the process of resolving issues during an incident. The teams should be careful not to violate the confidentiality of any individual or organization. Legal advice and guidance should be sought, as required or deemed necessary.

- Availability

Teams should get what is needed and when it is needed. For example, without having timely information for analysis, the teams cannot proceed and would need to stop at certain junctures of the incident response process. This can adversely impact the recovery of the affected constituent's business.

- Integrity

Teams should be sure the information stays the way it was intended. There must be inherent trust built between teams for the sake of information exchange and integrity of the information so that it remains untainted.

- Authenticity

Teams should know where the information is from and who the possible owner is. This is not always easy to know, but the CSIRTs must make a serious attempt to identify and record sources and ownership of the information each time it is received.

- Exclusivity

Teams should assure that only the intended recipients can use the information as specified. As stressed in the first article, building trusting relationships between teams is extremely important. This, of course, results from continued contact and agreement development and maintenance at various national-level and international-level organizations and agencies. A large organization of a multi-billion dollar enterprise could exert more pressure in establishing guidelines and specifications for information sharing and exchange than a smaller enterprise with a few million dollars in revenue. Intended recipients have a responsibility to process the information as specified and expected by the agreed on terms.

- Privacy

Teams should guarantee that the interests of persons and organizations are protected. Privacy laws are changing continuously in most of the progressive countries around the world. In addition, these laws differ from country to country. Certain information can be considered sensitive in one country, but not in

another (for example, a country that is a member of the European Union versus the United States). Careful planning, along with professional guidance, must be made in retrieving, storing, and transmitting such information.

- **Obligation**

Teams should guarantee that the due diligence requirements are fulfilled. There is an overriding, unwritten obligation to do the right thing for the benefit of all of the parties involved in servicing the incidents and the constituents. This means, for example, the use of required tools (such as encryption) with consideration towards export controls and regulations of the countries involved when information needs to cross national boundaries to reach another national-level CSIRT. In addition, although physical security needs attention, a CSIRT might not typically have full authority to implement all aspects of physical security because its parent organization usually has that authority. For instance, in the context of this article, a VCSIRT relies on the worldwide security team of the organization to possess such authority.

---

## Execution of an Incident Response

From here on, we cover the execution of security incident response policies for customers. Discovery and reporting of the incident is briefly covered in the beginning of the evaluation phase. In this article series, we focus primarily on five phases of response execution when a security incident is reported at the customer site:

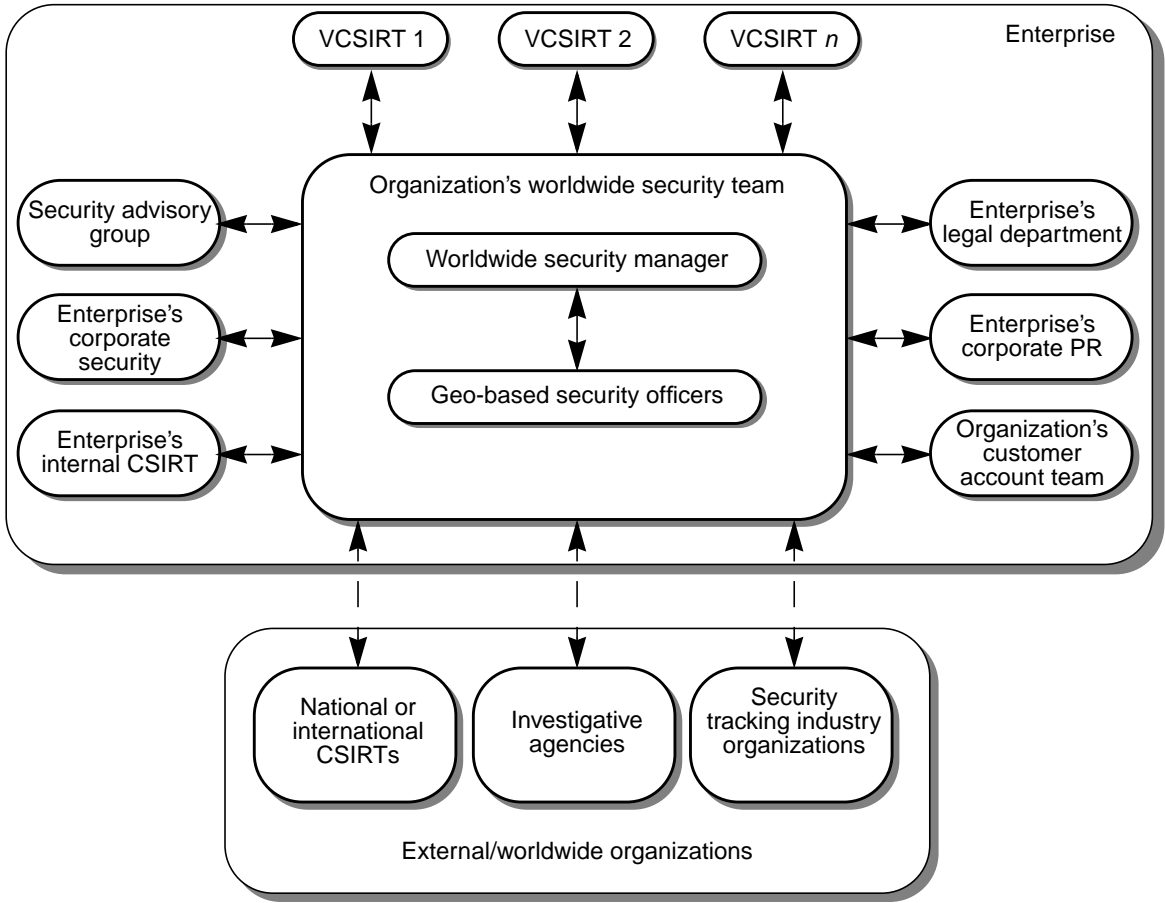
- Evaluation
- Containment
- Eradication
- Recovery
- Follow-up

Evaluation, containment, eradication, and recovery are discussed in this article. Following up after the recovery will be discussed in the next article.

In Figure 2, the relationships and communication between security and other related teams is summarized for an organization to prepare a plan for incident response and make decisions to execute the five phases. As described in the first article, the organization's worldwide security team has a worldwide security manager and security officers within it, based on the geographic area. Primarily, the organization's worldwide security team communicates with all of the other security teams, legal, and PR organizations to resolve incidents by creating VCSIRTs, as needed on a per

incident or more than one incident per site basis, as necessary, based on resources and urgency. The VCSIRTs have geographic jurisdiction assigned by the worldwide security team.

Also, in Figure 2, it is shown that worldwide security teams will need to work with national and international CSIRTs. For example, for Germany, DFN-CERT is the national CSIRT, and examples of international CSIRTs are AusCERT in Australia and CERT/CC in the U.S. In addition, it will be necessary, depending on the situation, to work with investigative agencies and security tracking organizations, such as SANS ([www.sans.org](http://www.sans.org)) and securityfocus ([www.securityfocus.com](http://www.securityfocus.com)). The communications with these external agencies might not be direct; the corporate security team or the enterprise's internal CSIRT might be involved.



**FIGURE 3** Communication Between the Organization's Security Teams, Enterprise's Teams, and External Security Teams and Agencies

---

## Evaluation of a Security Incident

Prepared policies and procedures, which include the necessary actions to observe systems and networks for signs of unexpected behavior (including intrusions), at the customer site help in the detection of a possible incident and the writing of a report. Observation involves monitoring, inspecting, and auditing the systems and networks. Evaluation is the next step.

The organization's geo-based security officer and that officer's staff should be responsible for the initial evaluation of any security incident, within the scope of that constituency. Evaluation starts with reviewing the report of an incident. Multiple reports might come in within short intervals of time. These reports should be consolidated with the help of the geo-based security officer's staff for the affected constituent, as designated by the worldwide security team. Also, in spite of the different possible ways of communication, points of contact and submission mediums regarding the incident should be standardized as part of the security policy (as discussed in the last article). Note that an incident could be reported by a non-technical person, so the report form could be partially completed in the initial submission. A security expert's help is necessary to complete the form after the initial submission. The following shows an example of a submission form.

Incident Response and Reporting Checklist	
1. Status	
<input type="checkbox"/> Site under attack <input type="checkbox"/> Past incident <input type="checkbox"/> Repeated incidents, unresolved	
2. Contact information	
Name: _____	Title: _____
Organization: _____	
Direct-dial phone: _____	Email: _____
Legal contact name: _____	Phone: _____
Location/site(s) involved: _____	
Street address: _____	
City: _____	State/province: _____ Country: _____
3. What is the nature of the emergency? (Check all that apply.)	
<input type="checkbox"/> Denial of service attack <input type="checkbox"/> Unauthorized electronic monitoring	
<input type="checkbox"/> Network intrusion <input type="checkbox"/> Insider attack <input type="checkbox"/> Probe/scan	
<input type="checkbox"/> Malicious code (virus, trojan horse, worm)	
<input type="checkbox"/> Website defacement	
<input type="checkbox"/> Other (please explain) _____	
4. Date: _____	Time: _____
5. Duration of attack: _____	
6. Impact of attack	

Loss or compromise of business data? \_\_\_\_\_  
System downtime: \_\_\_\_\_  
Damage to systems: \_\_\_\_\_  
Financial loss: \_\_\_\_ (estimated amount: \_\_\_\_\_)  
Damage to the integrity or delivery of critical goods, services, or information \_\_\_\_\_  
\_\_\_\_\_  
Other organizations' systems affected: \_\_\_\_\_  
\_\_\_\_\_  
7. Severity of attack (include financial loss) \_ low \_ medium \_high  
8. Did the attacker gain root, administrative or system access? \_\_\_\_  
9. How was the incident detected?  
\_ Intrusion detection system or audit logs  
\_ External complaint  
\_ User report  
\_ Other: \_\_\_\_\_  
10. What are the known symptoms? \_\_\_\_\_  
11. What business areas are affected? \_\_\_\_\_  
12. What systems are affected? \_\_\_\_\_  
(Gather as much information as possible about the systems, including suspected systems. For instance, gather the name of the operating system, platform, applications, IP address, associated or suspected user IDs, most recent changes applied, and other related items, as you deem pertinent.)  
13. Are the systems still connected to the internal network? \_\_\_\_  
14. Are the systems still connected to the Internet? \_\_\_\_  
(Consider disconnecting the systems, if possible.)  
15. Are the backups of the perceived affected systems available? \_\_\_\_  
(Provide all of the information regarding online, onsite, or offsite backups.)  
16. Are the affected systems still at risk or attack? \_\_\_\_  
(Consider disconnecting the systems or securing the accounts, if possible.)  
17. Will the systems potentially require forensic analysis? \_\_\_\_  
(Consider shutting down and securing the system for forensic imaging.)

## Determining If an Incident Is Real

The first task is to determine if the security incident is *real*. Why? Because, a large percentage of incidents are false alarms. As the first step upon the notification of an incident, the organization's worldwide security team must make every attempt to reduce panic on the affected constituent's behalf. The organization's geo-based customer account manager, who is responsible for the site in question, should

deploy the organization's resources to determine if the incident qualifies as a security incident by consulting with the security officer responsible for the geographic area.

## Clarity of the Notification

Clarity of communications regarding an incident impacts the ability to determine if an incident is real. In the first article, necessary policy statements were mentioned regarding these communications. FIRST has a document (contributed by AusCERT) that defines how to communicate internationally, limiting confusion (refer to [http://www.first.org/docs/international\\_comms.html](http://www.first.org/docs/international_comms.html)).

VCSIRTs must follow these suggestions that cover many topics, such as currency, postal codes, measurements (metric or imperial), time formats and zones, seasons, telephone numbers, and so on.

## Trusting the Source of the Notification

Another factor that significantly contributes to the reality judgment is trust. If you do not know the source of notification well, it is difficult to assess the quality and relevance of the contents of the notification of an incident. For example, if your team receives information about a potential new *Internet worm* from CERT/CC in the U.S. or AusCERT in Australia, it is likely you will pay considerably more attention to it than if it had been received from an unknown, or lessor known, source or from an individual.

## Detection of an Incident

Detection implies and embraces potentially a much wider range of incidents than just intrusion detection. For instance, a virus infection can be found using specific detection techniques, but not by intrusion detection tools. Also, depending on the type of intrusion detection (for example, network-based versus host-based), an insider host-level misuse (or what can be defined as a violation of the security policy), resulting in a security incident, might not be noticed.

CERT/CC offers an intruder detection checklist that outlines suggested steps for determining if your system has been compromised (refer to "Intruder Detection Checklist" at: [http://www.cert.org/tech\\_tips/intruder\\_detection\\_checklist.html#A1](http://www.cert.org/tech_tips/intruder_detection_checklist.html#A1)).

The following list contains some of the typical symptoms:

- Unusual log file entries (although expert intruders are good at covering their tracks, examples include new accounts, numerous failed login attempts, and logins into dormant or default accounts)
- Presence of new `setuid` or `setgid` files
- Changes in system directories and files
- Unusual hidden files or ambiguous files, such as those from past incidents (for example, `/tmp/bob` and `/etc/inet.d`)
- Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server (these are usually the most obvious signs of a compromised Web server)
- Accounting discrepancies
- Suspicious probes (for example, login attempts) and browsing
- Activity during non-working hours or holidays
- Presence of cracking utilities (for example, Crack), which might have been loaded by an authorized user with bad intentions
- Unaccounted for changes in the DNS tables, router rules, or firewall rules
- Unexplained elevation or use of privileges (for example, gaining superuser privileges)

---

**Note** – Clever intruders tend to not use the superuser logins because they attract attention. Instead, they prefer to use raised privileges of a normal user.

---

- System crashes  
Crashes could be due to a planned denial-of-service attack or due to an amateur hacker stumbling out of a system in a hurry, leaving it in a hung or crashed state.
- Unexplained poor system performance  
In the case of poor performance, care should be taken because it is difficult to determine that the system has been compromised just because it is performing poorly.
- Failed or successful social engineering attempts (for example, attempts to obtain a network password over the phone by someone pretending to be an employee)

System administrators and security engineers deployed by the VCSIRT at the affected constituent site can use this information to look for and confirm several types of break-ins. Tools, such as Tripwire and MD5 signatures, can help you determine changes in system files and, in turn, provide clues about the actions of attackers and confirmation of a compromise.

For more information about Tripwire, refer to:  
<http://www.sun.com/software/security/tripwire>

The Solaris Fingerprint Database Companion, `sfpc`, automates the process of collecting and checking MD5 signatures against the Solaris Fingerprint Database, `sfpdb`.

The Solaris Fingerprint Database Sidekick, `sfps`, simplifies the process of checking for the presence of rootkits on the compromised system, which is a sign that an intruder has broken into the system.

---

**Note** – Rootkits are sets of modified system binaries that provide hackers with hidden backdoors that enable future access to compromised systems.

---

The Solaris Fingerprint Database Sidekick accomplishes the detection of rootkits by maintaining a list of common trojan-horse software that is intentionally modified with a malicious intent (for instance, Solaris OE executables such as `/usr/bin/login` or `/usr/bin/passwd`).

For more information about these tools, refer to:

[http://www.sun.com/blueprints/tools/fingerprint\\_license.html](http://www.sun.com/blueprints/tools/fingerprint_license.html)

## Determining the Scope

After the incident is qualified as real, the scope of the incident should be quickly determined. The customer account manager should assemble the appropriate field engineer (for example, the organization's field engineer at the site in question or a technical support engineer from the customer service center that is servicing the site) and engineering resources (for example, the organization's security engineer or forensic expert) and work with the security officer to answer the questions in the following two sections. If the security officer for the geographic area in question is not available, then the worldwide security manager should assign another officer.

### General Scope Questions

The following list contains general questions that should be asked to determine the scope of the incident:

- Is there just one, or more than one, incident involved simultaneously?
- Is this a single site or a multisite incident?
- Is this a single geo or multi-geo incident (considering that businesses are generally divided into several geographic sub-entities)?
- Is sensitive information involved?
- What is the entry point of the incident (for example, the network, the phone line, or other)?

- What is the potential damage of the incident?
- What is the estimated time to close out the incident?
- What resources are required to handle the incident?
- Will the press be involved?
- Should law enforcement be involved?

Answering these questions facilitates the deployment of a proper plan and the resources to mitigate the damage and to restore business operations. After the plan is ready, it should be communicated immediately to the organization's worldwide security manager by the organization's geo-based security officer from the geographic area where the incident took place.

## Detailed Scope Questions

More detailed questions should be discussed as experts are engaged by the security officer for the affected constituent. These questions include:

- What is at risk?
  - Are applications, middleware, or databases at risk? The higher the number of components affected, the wider the scope of the incident and investigation is.
- Was one or more systems affected by the incident?
  - The more systems affected, the wider the scope is. Different intervention methods are generally required as the scope widens.
- Was one or more networks affected?
  - As with the case of systems, the more networks involved, the broader the scope is, and the greater the need is for immediate and urgent action.
- How far into the internal network did the intruder(s) get?
- What network segments were affected?
  - If a host outside of the security perimeter was affected (for example, on the DMZ), the intensity of the loss could be less than the loss for an internal network host inside of the security perimeter. (The DMZ, or "de-militarized zone," is the network added between a protected network, such as an internal network for the constituent's enterprise, and the external network, which is usually the Internet. The DMZ provides an additional layer of security and typically houses externally reachable services that cross a firewall, such as services provided by domain name servers and Web servers.)
- Who knows about the incident?
- To what extent does the knowledge of the incident make it worse?
  - PR and legal departments for the constituent, as well as for the servicing organization, should be concerned about the answers to these last two questions.

---

## Containing the Incident

After the security compromise is discovered and identified as real, the next step is containment. Containment involves limiting the extent of the attack, making key decisions, and executing predetermined (yet customizable) procedures. The goals at this stage could also include identifying the intent of the attack. For example, is this a malicious attack, or is the intruder just browsing to plan for future attacks?

### Limiting the Extent of an Attack

Two of the most fundamental objectives are to restore control of the affected systems and to limit the impact and damage to the customer's business. In the worst case, shutting down the systems or disconnecting the systems from the Internet (or from the source of the security problem, if known) could be the only practical solution. The following table contains examples of possible containment tactics.

Tactical Action	Description
Increasing the level of monitoring	This action involves actively tracking traffic for unusual activity (for example, port scanning) or patterns of an attack stream of bits, bytes, or packets.
Changing the filtering rules of firewalls and routers	This action excludes traffic from hosts that appear to be the source of an attack.
Disabling known vulnerable services, such as file transfer or calendar services	This action is effective when newly discovered service vulnerabilities are exploited by attackers.

Tactical Action	Description
Setting up traps	This action involves learning the intruder's identity or modus operandi (MO). The MO is a mechanism by which the perpetrator commits his or her crime. It is a learned behavior and can change over time. An MO can be considered a pattern, allowing for some variance. Examples of traps are honeypots (that is, computers designed to attract attackers in order to record their behavior and to gather evidence, but not meant for legitimate users), automated message systems that track unusual usage of a system or an application, and trojan horse commands (in this context, an intentionally modified command to deceive the intruder who might believe that the command is a <i>normal</i> command). For example, on UNIX systems, you can use the <code>finger(1)</code> command to display information about local and remote users, the <code>rwho(1)</code> command to display who is logged in on local machines, and the <code>nslookup(1M)</code> command to query Internet domain name services interactively. Refer to the UNIX man pages for these commands for more information.
Shutting down systems	This action might appear drastic, but it is sometimes advisable, usually based on a decision to prevent further loss and/or disruption. This is, of course, a joint decision between the constituent and the VCSIRT responding to the incident, with the geo-based security officer representing the servicing organization involved in the decision.
Disconnecting a system from the network	Although some disruption is unavoidable, users should still be able to use some local services. Be careful. The network might involve wireless local area networks (WLANs). In these cases, it might be important to disable and/or remove the wireless access points from the internal network. (WLANs are communication networks that use radio frequency technology to transmit network messages through air within a single location, such as an office or a university.)
Retaliating against the attacker	There might be a temptation to retaliate against the system originating the harmful traffic. However, you should avoid this temptation due to possible legal complications. Consult with management and legal representatives if there is such a desire. For instance, the system used by an attacker could be just a launching pad for the attack and belong to an innocent party.

## Making a Decision

The organization's geo-based customer account manager, in conjunction with the geo-based security officer, should make a decision for containment. Risking temporary, limited damage for determining the root cause is sometimes necessary. Pros and cons should be noted by the security officer's staff for the *Lessons Learned* documentation.

Schemes exist for selecting the most important incident or for ranking several incidents (if they occur in relatively close intervals of time). The following table contains a list of criteria (this list is not sequential).

Criterion	Description
Resources needed to deal with the incident	Forensic experts might be needed immediately to analyze a major incident versus simply disconnecting the compromised equipment from the Internet for later analysis.
Impact on constituency	Customers might be sensitive, based on the intensity level of the intellectual property loss. It could be a violation of privacy legislation versus a serious theft of software property, critically affecting a customer's enterprise-level business.
Type of incident	Is it just a break-in on the part of the intruder with the intention of performing a reconnaissance mission or a serious denial-of-service attack?
Type or extent of the damage	This could range from the loss of production for a couple of hours to a total shutdown of a site and exposure to media with a constituent's reputation as a service provider at risk.
Target or source of an attack	Is the target a large well-known enterprise or a small business? Is the source known from past incidents?

Expect exceptions to the selected scheme, so flexibility is key to accommodating them in the policy execution.

## Executing Predetermined Procedures

Predetermined, detailed procedures should be executed to contain the incident. These procedures are defined and created by the organization's worldwide security team, with the SAG's advice and review, for VCSIRT usage and distributed during formal training to the organization's security personnel by the worldwide security team. Predetermined does not necessarily mean noncustomizable. As per the situation, changes to these procedures should be expected, but a process must be in place to oversee and record those changes, under the supervision of the designated geo-based security officer.

---

## Eradicating the Incident

Eradication essentially means ending the intruder's attack on the customer's system. It can be achieved by turning off the affected system and network (if known) and/or disconnecting from the Internet, as well as from the rest of the internal network at the customer site. Secondly, eradication involves restoring systems to a secure baseline configuration. This step should not be underestimated by the VCSIRT or its counterparts acting on behalf of the VCSIRT at the customer site. A major incident, or multiple almost simultaneous incidents, can cripple a large site with hundreds or thousands of computers or computer-based equipment. Sometimes, the best way is to completely erase and rebuild the system from scratch. But, that is not always practical from the following points of view:

- The time and complexities involved in performing a rebuild
- The trust involved in the components used for restoration by the VCSIRT or their representatives at the affected constituent's site

According to ITU-T X.509, Section 3.3.54, *trust* is defined as follows: "Generally an entity can be said to trust a second entity when the first entity makes the assumption that the second entity will behave exactly as the first entity expects."

- The procedures that must be executed to preserve the evidence of the intrusion or attack before valuable forensic data left by the attackers on hard drives or in core memory is erased. (This topic, along with chain-of-custody aspects, will be discussed in detail in the next article of this series.)

When doing a complete rebuild, the constituent must be advised of trusted sources (for example, CD-ROMs or trustworthy locations providing guarantees of downloaded contents through methods such as message digests—for example, MD5 checksums). For more information on message digests, refer to:

[http://www.sun.com/blueprints/tools/fingerprint\\_licence.html](http://www.sun.com/blueprints/tools/fingerprint_licence.html)

In addition, the constituent should be guided in the use of state-of-the-art software tools and a clean backup to remove or mitigate damage and to keep a safe copy for future use when the system usage is resumed.

But, what assurance is there that the backup would be clean when the system or network resumes its operation? Every site does not have the best tools, expertise, or time at hand to remove malicious code (such as worms and viruses) and to research and patch vulnerabilities. That is why it is important that the organization assisting its constituent customers provides the best possible tool set or proactively makes sure the customers have adequate tools to perform recovery from an incident. Otherwise, the customers might be setting themselves up for a future incident or for a repeat incident of the same kind.

## Common Indicators of UNIX System Intrusions

In spite of repeated publicity at several well-known Web sites by the security coordinating industry organizations, even the most commonly known vulnerabilities are not addressed by a large percentage of sites. The following list contains common indicators of UNIX® system intrusions. The list is not all-inclusive. Attempted or successful intrusions might not have left obvious evidence. Use all resources available to analyze suspicious or suspected activities.

### ■ Binaries

If an intruder has gained unauthorized access to your system, quite often the intruder will try to replace or alter one or more of the binaries in the following list. This is a sample list only. The goal of the hacker is mentioned in parentheses for some of the example files:

- `/bin/df`
- `/bin/ls` (to hide logs and files that can provide clues to intrusions)
- `/bin/login` and `/sbin/login` (to provide login backdoors)
- `/bin/ps` (to hide processes that provide online clues of hacker processes—for example, password-cracking utilities)
- `/usr/etc/in.telnetd` (to provide network backdoors—for instance, trojan-horse versions of Telnet that provide a root shell when a particular value is set for TERM)
- `crontab` (to hide scheduled jobs that steal passwords or cleanup logs)
- `/usr/sbin/ifconfig` (to provide a trojan-horse `ifconfig` file that hides the use of the promiscuous mode of network interfaces, which is used by sniffers to identify passwords)
- `/usr/ucb/cc`
- `/usr/ucb/netstat` (to hide unauthorized connections)

### ■ File modifications

The intruder might attempt to modify one or more of the following critical files:

- `.cshrc`
- `.forward`
- `.login`
- `.profile`
- `/.rhosts`
- `/bin/.rhosts`
- `/etc/hosts.equiv`
- `/etc/group`
- `/etc/passwd`

- Hidden directories

Intruders often attempt to hide files in one or more of the following directories:

- `/etc/tmp`
- `/tmp`
- `/var/tmp`
- `/usr/lib/cron`
- `/usr/spool`

## Common UNIX System Configuration Issues

The following list contains commonly known and exploited UNIX configuration issues that translate into a *not-to-do* list on rebuild or on resumption of operations. (These are more or less self-explanatory, having been announced in vulnerability notices over the years, and available at public sites in various forms, but a brief description is provided here.)

- Poor passwords

- Weak passwords (that is, nouns or words used from dictionaries) should not be used as passwords. There are well-known rules of password construction (for example, using combinations of alphabetic characters—upper and lower case, 0-9 digits, and punctuation marks).
- Accounts with default passwords should not be used (for example, vendor supplied ones). Scan your password file for extra UID 0 accounts.
- Reusable passwords should not be used. At the very least, a single password should not be used for multiple accounts. It is common for intruders (who might be *camped out* on the internal network) to harvest (as in, clear-text) user name and password information using packet sniffers from a subnet, a local physical network, or a wireless network.

- Use of TFTP (Trivial File Transfer Protocol) to obtain password files

Disable `tftpd`. If you need to have it, design restricted access. If your constituent suspects that passwords have been stolen, then of course, change all of them.

- Vulnerabilities in `sendmail(8)`

Numerous vulnerabilities have been found in `sendmail`. The `sendmail` restricted shell (`smrsh`) controls the way mail messages can interact with the operating system. `mail.local` can be used to control the way `/bin/mail` is used on the system.

- Misconfigured anonymous FTP

You should not use your system's standard password file or group file as the password file or group file for FTP. Also, the anonymous FTP root directory and its two subdirectories should not be owned by FTP.

- Inappropriate network configuration file entries
 

Watch out for this common vendor mistake (`/etc/hosts.equiv` with a `+` sign entry). The `+` sign indicates that your system trusts all systems.
- Inappropriate *secure* settings in `/etc/ttys` and `/etc/ttytab`

The only terminal that should be set to secure should be the console.
- Inappropriate entries in `/etc/aliases` or `/usr/lib/aliases`

Remove entries such as `uudecode`, if they are not yours. These entries are setups for hackers.
- Old versions of system software
 

When to patch is a common issue for system or network administrators, generally due to lack of time or resources. Thus, this type of faltering opens doors for attackers. It is argued by theorists that ideally, the best time to patch is not when the patch first comes out from the vendor because it could have new bugs or there could be a vendor recall due to other business reasons. However, the wait introduces an element of risk.
- Use of `setuid` shell scripts
 

`setuid root` shell scripts are a potential security risk.
- Inappropriate export settings
 

Use `showmount` to verify `/etc/exports` files. Watch out for examples, self-reference of NFS server, export file systems to hosts (with fully qualified host names) that are known to require them. For further details, refer to:

`ftp://infor.cert.org/pub/cert_advisories/CA-94:15:NFS.Vulnerabilities`
- Vulnerable protocols and settings
 

Consider filtering certain TCP/IP services at your site boundary firewall and router. For further details, refer to:

`ftp://info.cert.org/pub/tech_tips/packet_filtering`
- Inappropriate file and directory protections
 

Systems with these can be a hacker's paradise. Use the vendor's system documentation to verify that system files and directories have correct protections and ownership (in particular, the root, `/`, and `/etc` directories).

Many guidelines exist for recovery from root compromises. For more information refer to CERT/CC:

`http://www.cert.org/tech_tips/intruder_detection_checklist.html#B2`

While following the guidelines provided at public sites, such as above, VCSIRTs must keep their parent organization's policy in perspective.

## Capturing Evidence Before Cleaning Up

The compromised system cannot be trusted under any circumstance. System binaries, configuration files, and even the system's kernel might have been modified by the attacker(s). For example, after compromising a machine, attackers, especially in UNIX systems, install programs called *root-kits* that allow them to regain access and to cover their tracks, as in removing entries from system logs. There might be pressure from the constituent's management to get the system back online, but you must follow a process (defined in the policy) to preserve the data on the compromised system for a later analysis, which can be time-consuming. Great care must be taken to collect all of this necessary information because it can be lost in the process of cleaning up the system's hard drives and core memory. If bogus files and attacker's toolkits have been created or left behind by an intruder, archive them before deleting them.

All further analysis should be done on a trusted copy (which was previously built and physically secured), not on the original compromised system. Many times, it might be deemed necessary to leave the compromised system online to collect all of the proof of an attack, but a note of caution here is that there is a possibility that the attacker could regain control, again and again, while you are recovering the system, handing you setback after setback. On the other hand, if you have support from the constituent's management team, and you are a forensic expert with the intention to capture the attacker by learning his or her behavior, then this is an opportunity. (This topic will be discussed in detail in the next article.)

There are three types of tools (or operating system commands) available in UNIX and Linux for backups:

- Tape archive: `tar -flags device file_system_to_be_dumped`
- dump (the primary backup program): `dump -flags device file_system_to_be_dumped`
- Device-to-device copy: `dd if=input_file output_file`

For details, check the man pages on your UNIX or Linux system. Note that in most Linux systems, a dash (-) does not appear before any flag. Making a full backup of the victim system immediately when it appears that an incident has occurred is very important. The `dd` tool can read files that are submitted to it as inputs on a block-by-block basis. Thus, it can capture data, such as deleted blocks, that `tar` and `dump` cannot. For detailed guidelines on the use of the `dd` tool, refer to:  
<http://www.crazytrain.com/dd.html>

Never reuse the system backup of a compromised system because it might reintroduce a bug into the production environment. Later, you might have to reload certain portions of the saved environment, but anything you get from the vendor's distribution media (for example, operating system and associated system binaries) should not be restored from the backed-up disks during the recovery phase.

## Using State-of-the-Art Software Tools

Software tools, such as antivirus software, should be available within an enterprise to eradicate damage. A number of public sites are available to download freeware tools. However, care must be taken not to accidentally use tainted software. We could provide a long list, but undoubtedly, many of the tools will be surpassed or become obsolete in the course of time. A sad fact is that there are few security conscious applications currently available. Primarily, this is caused by the need for a sound security infrastructure that must be put in place first for most tools to run on securely. The following list contains a few locations. Be sure to use a well-known mirror of these sites:

- CERT/CC at: `ftp://info.cert.org/pub/tools`
- DFN-CERT at: `ftp://ftp.cert.dfn.de/pub/tools/`
- Purdue University's Computer Operations, Audit, and Security Tools (COAST) at: `coast.cs.purdue.edu/pub/tools`
- Sun BluePrints™ Scripts and Tools Web site at:  
`http://www.sun.com/blueprints/tools/`

The `netcat` tool is an extremely useful utility for transferring information over TCP or UDP. Be certain that your VCSIRT has the authority to install and use `netcat` on your customer's network. For details on using `netcat`, refer to the following sites:

- `http://www.sans.org/rr/audit/netcat.php`
- `http://www.insecure.org/tools.html`

Copying images from compromised systems to the safe (that is, trusted) system can be accomplished with `netcat` listening on the trusted system, while running trusted `dd` from the vendor's CD-ROM that is mounted on the compromised system. For analyzing the UNIX system, the recommended tool is The Coroner's Toolkit (TCT). TCT is a suite of tools. For more information, refer to:  
`http://www.porcupine.org/forensics`

---

## Recovering From an Incident

Recovery is often regarded as an urgent step to reduce the customer's business losses due to downtime. Recovery involves returning the system to normal by using a predetermined checklist. The checklist might not be a set of hard-and-fast rules. Human intervention is a key element and is why a checklist should be treated in the policy as a flexible process tool. It is only a set of guidelines for the VCSIRT members during the execution of the policy.

## Returning the System to Normal

Bringing business back to normal operations with minimal user inconvenience is critical, particularly when customer systems are involved. All of the organization's personnel, under the supervision of the organization's security officer for the geographic area in question, must keep this in mind as the highest priority after an incident.

One of the surest ways to recover is to perform a full-system restore from a trusted media, but the main question is was the media used for restoration purposes adequately safeguarded at all times. It is also time-consuming and difficult if multiple systems were compromised. It is extremely important to note here that a full restore, including changes to every password, is mandatory if an intruder gained superuser access to systems and/or networks.

Recovering data is critical to your constituent's business, but it is also very tricky. You should keep the following in mind:

- You can restore data from the last full backup, even if this is not the most perfect solution. You can also use incremental backups, if there were modifications since the last full backup.
- You can use fault tolerant storage system hardware, such as RAID, to recover the mirrored or striped data that resides on the redundant hard drives.
- You might have to use offsite, safeguarded storage if all of the equipment was compromised. The data might not be current if the last backup was several days or weeks old, which would impact the business; however, this is the real cost for not having fault redundancy in the storage design, secured offline storage, or highly-secured, locked-up storage on site.

Recovery of classified computing systems (as in the case of the U.S. Government) is outside the scope of this article, but in the U.S., note that the government agency that has jurisdiction over the geographic area in which the constituent resides needs to be contacted. For example, in the New York area, there is NYCTF (New York Electronic Crimes Task Force), which is part of a conglomeration of regional task forces known as Electronic Crimes Task Forces (<http://www.ectaskforce.org>).

In the northeastern states of New England, there is the New England Electronic Crimes Task Force (NET). There are also equivalent organizations in the San Francisco Bay area, Chicago, Las Vegas, Los Angeles, Charlotte, and Miami.

In the case of a disaster, such as a highly destructive network intrusion, priority schemes and escalation procedures should be followed, such as what to do first and whom to warn before attempting to bring the customer site back to normal. The VCSIRT must take proper precautions to provide backups. Key sets of processes and guidelines for disaster recovery will be presented in a future article.

Much of the process development must take place in the incident preparation stage, as described earlier. The maturity of the process design usually takes place in the post-established phase of the worldwide security team. This is discussed in a future article in this series.

The recovery process, occurring after the preservation of the evidence of an attack and the restoration of a secured clean backup, needs involvement by and guidance from a forensic expert that must be engaged by the organization's geo-based security officer. This person will be able to confirm that the eradication, and all of the necessary post-attack data gathering, was successful. The determination of success could also be a team decision involving the forensic expert.

## Predetermined Checklist

A predetermined checklist (developed and distributed by the organization's worldwide security team for verification) should be used to confirm the return to normalcy before turning the system online or connecting to the Internet. The checklist should serve only as a guideline because it cannot anticipate all situations. Security experts in the geo-based security officer's VCSIRT should judge the validity of each step before executing it. At a minimum, the following broad areas of responsibilities must be considered, beyond what has already been stated.

---

**Note** – The following table cannot be considered a complete checklist of responsibilities. It is just a sample.

---

Recovery Actions	Description
Formally recording all actions	All actions must be recorded, including the dates and times (in total) required for each person on the VCSIRT.
Periodically notifying users of status	You must keep all of the users of the constituent's customer site informed of the status of the recovery. Business critical issues can be addressed simultaneously by the customers, based on the status reports.
Advising on major breakthroughs, setbacks, or developments	If any major breakthrough or development takes place during the course of recovery, it is the responsibility of the organization's designated security officer to communicate it clearly, yet cautiously, to the constituent's business operations management on behalf of the VCSIRT. All recoveries are not successful. Setbacks should be expected and must be recorded for the <i>lessons-learned</i> documentation. They should also be communicated to the constituent and the VCSIRT.

Recovery Actions	Description
Adhering to security incident response policy (SIRP) guidelines	As much as possible, the VCSIRT must follow the SIRP guidelines. For example, it must seek legal and PR guidance to protect itself from any liability or undesirable media coverage that can adversely affect the constituent's business.
Patching vulnerabilities and minimizing and/or hardening the system	<p>Patching must be done thoroughly at all levels of software, from operating systems to middleware to applications. Patching vulnerabilities must take place for compromised systems, as well as for systems that were unaffected by the attack, especially those that are not up-to-date. The latter is important because they could be the targets of attackers the next time.</p> <p>Minimization is the process of removing unnecessary components. (Patching could happen during this process.) The process reduces the number of components to be hardened, patched, configured, and/or reconfigured. Although the process of determining the minimized configuration is time-consuming, removing the components is worth the time because they are generally the most susceptible targets (for example, external Web servers, firewalls, directory servers, and domain name servers). For guidelines on minimization, refer to: <a href="http://www.sun.com/blueprints">http://www.sun.com/blueprints</a></p> <p>Hardening the disks against past, and possible future, attacks must be considered. This might mean disabling certain services and modifying configuration files. Vendor packages and scripts might be available (for instance, Sun's Solaris™ Security Toolkit at <a href="http://www.sun.com/software/security/jass/">http://www.sun.com/software/security/jass/</a>).</p>
Removing any interim measures	Administrators use <i>stop gap</i> measures for short-term containment. These measures must be removed before bringing the customer site or system back on line. Examples of such measures are turning off Telnet on tcp port 23 or FTP on tcp ports 20 and 21.
Announcing the completed recovery	At this point, there must be an overall determination (even if a detailed forensic analysis has not been completed) as to how the security was breached and if required reinforcements have been made, before returning the systems to service. It must be the responsibility of the designated geo-based security officer to perform the final check before announcing to the constituent that the system or site is back to normal operation.

---

## Article Series

The “Responding to a Customer's Security Incidents” articles are an on-going series. The next article will cover best practices for following up after the recovery from a security incident. It will discuss postmortem analysis, legal, investigative, and

government recourses, gathering evidence, and postincident procedures—two of the most important being capturing lessons learned and performing risk analysis—to be executed by the enterprise's organization for its affected constituent.

---

## 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 (specifically, enterprise and Internet-level, highly available, 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 and UNIX, the Solaris OE, and TCP/IP-based network and security technologies, services, software products, and development tools. He represents Sun in several industry forums. He is invited often 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, Engineering, and Sun Corporate and IT Security for reviewing this article and providing helpful comments (in particular, Joel Weise, Martin England, Glenn Brunette, Matthias Kussinger, and Scott Elam)
  - Sun BluePrints personnel who contributed in editing and revising this article
- 

## References

The following references were used to write this article:

- Brazilian National Research Network, "References on Network Security and Network Security Teams in Brazil,"  
[http://www.rnp.br/cais\\_en/cais-referencias.html](http://www.rnp.br/cais_en/cais-referencias.html)

- Beattie, S., et al., "Timing the Application of Security Patches for Optimal Value," Proceeding of LISA '02: Sixteenth Systems Administration Conference, Berkeley, CA, USENIX Association, 2002
- CERT, Software Engineering Institute, "CSIRT FAQ," Carnegie Mellon University, 2002, [http://www.cert.org/csirts/csirt\\_faq.html](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
- DFN-CERT, Germany, "Glossary of Computer Security Incident Handling Terms and Abbreviations," September 2002, <http://www.cert.dfn.de/eng/pre99papers/certterm.html>
- EICAR, European Institute of Computer Anti-Virus Research, <http://www.eicar.org>
- Fraser, B., ed. *Site Security Handbook*, RFC 2196, Internet Engineering Task Force, September 1997
- ITU-T Recommendations X.509, ISO/IEC 9594-8: "Information Technology - Open Systems Interconnection - The Directory: Public Key and Attribute Certification Frameworks"
- Masurkar, Vijay, "Responding to a Customer's Security Incidents (Part I): Establishing Teams and a Policy," Sun BluePrints OnLine, March 2003, <http://www.sun.com/blueprints/>
- Noordergraaf, Alex, *Enterprise Security: Solaris Operating Environment*, Sun Microsystems Press, Prentice Hall, 2002
- Rude, T., "DD and Computer Forensics," <http://www.crazytrain.com/dd.html>
- Shultz, E., and R. Shumway, *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*, New Riders Publishing, November, 2001
- Sun Microsystems, Inc., Solaris Security Toolkit, <http://www.sun.com/software/security/jass> and <http://www.sun.com/blueprints/tools>
- Sun Microsystems, Inc., "The Solaris Fingerprint Database - A Security Tool for Solaris Operating Environment Files," 2003
- United States of America's Federal Computer Incident Response Center (FEDRIC), <http://www.fedric.gov/>

---

## Ordering Sun Documents

The SunDocs<sup>SM</sup> 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`

