Organizing A Computer Security Incident Response Capability

PRACTICE OBJECTIVE

Organizing an effective computer security incident response capability (CSIRC) involves several major decisions and actions. One of the first considerations should be to create an organization-specific definition of the term "incident" so that the scope of the term is clear. The organization should decide what services the incident response team should provide, consider which team structures and models can provide those services, and select and implement one or more incident response teams. Incident response policy and procedure creation is an important part of establishing a team, so that incident response is performed effectively, efficiently, and consistently. The policies and procedures should reflect the team's interactions with other teams within the organization as well as with outside parties, such as law enforcement, the media, and other incident response organizations. This practice provides not only guidance that should be helpful to organizations that are establishing incident response capabilities, but also advice on maintaining and enhancing existing capabilities.

PRACTICE TUTORIAL

Need for Incident Response

Incident response has become necessary because attacks frequently cause the compromise of personal and business data. Malicious code incidents such as the SQL Slammer worm, the Blaster worm, and the Love Letter worm have disrupted or damaged millions of systems and networks around the world. Heightened national security concerns are also raising awareness of the possible effects of computer-based attacks. These events—and many more—make the case daily for responding quickly and efficiently when computer security defenses are breached. To address these threats, the concept of computer security incident response has become widely accepted and implemented in governments, private sector and academia.

The following are benefits of having an incident response capability:

- Responding to incidents systematically so that the appropriate steps are taken
- Helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information, and disruption of services
- Using information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data
- Dealing properly with legal issues that may arise during incidents

PRACTICE WORKBENCH

This practice workbench (see Figure 1) is designed to define management's policy for incident reporting, create an incident response team and assign that team specific incident reporting responsibilities.

The workbench commences with the recognition that a security incident response team is needed, then goes through a four step process to create that team and that at the conclusion of those four steps there will be a practice for security incident response directed by a team.

The four steps begin with defining what a security event is and what a security incident is. Based on this definition the second step writes management policy on incident response. The third step organizes the team and the fourth step determines team responsibilities other than pure incident response.

INPUT PRODUCTS

The growing emphasis on effective security measures necessitates the requirement that incidents are responded to in a formal manner. The difficulty facing many security systems is that when a security incident occurs there is no defined process for handling that incident. Thus, the only input needed for this work practice is the recognition that a formal incident response approach is needed.

IMPLEMENTATION PROCEDURES

This work practice to organize a computer security incident response capability has the following four steps:

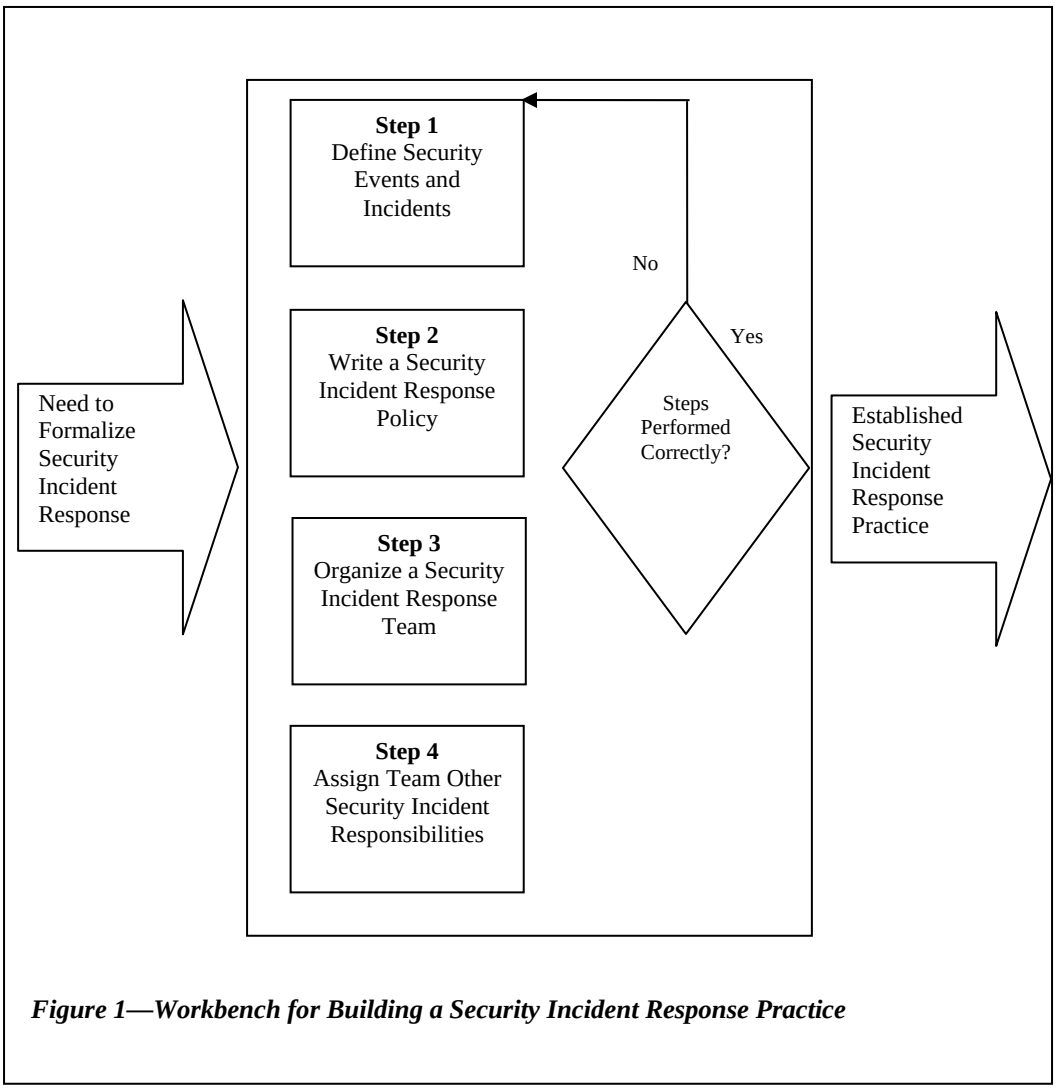

Figure 1—Workbench for Building a Security Incident Response Practice

Step 1: Define Security Events and Incidents

An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a Web page, a user sending electronic mail (email), and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a Web page, and execution of malicious code that destroys data. This guide addresses only adverse events that are computer security-related and excludes adverse events caused by sources such as natural disasters and power failures.

The definition of a computer security incident has evolved. In the past, a computer security incident was thought of as a security-related adverse event in which there was a loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. New types of computer security incidents have emerged since then, necessitating an expanded definition of an incident. An incident can be thought of as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of today's incidents are as follows:

- *Denial of Service (DOS)*
  - An attacker sends specially crafted packets to a Web server, causing it to crash.
  - An attacker directs hundreds of external compromised workstations to send as many Internet Control Message Protocol (ICMP) requests as possible to the organization's network.
- *Malicious Code*
  - A worm uses open file shares to quickly infect several hundred workstations within an organization.
  - An organization receives a warning from an antivirus vendor that a new virus is spreading rapidly via email throughout the Internet. The virus takes advantage of vulnerability that is present in many of the organization's hosts. Based on previous antivirus incidents, the organization expects the new virus will infect some of its hosts within the next three hours.
- *Unauthorized Access*
  - An attacker runs an exploit tool to gain access to a server's password file.
  - A perpetrator obtains unauthorized administrator-level access to a system and then threatens the victim that the details of the break-in will be released to the press if the organization does not pay a designated sum of money.

- *Inappropriate Usage*
  - A user provides illegal copies of software to others through peer-to-peer file sharing services.
  - A person threatens another person through email.

Step 2: Write a Security Incident Response Policy

This section discusses policies and procedures related to incident response, with an emphasis on interactions with outside parties, such as the media, law enforcement agencies, and other incident reporting organizations.

Policy governing incident response is highly individualized to an organization. However, most policies include the same key elements, regardless of whether the organization's incident response capability is indigenous or outsourced:

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and their consequences within the context of the organization
- Organizational structure and delineation of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, and the requirements for reporting certain types of incidents
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms

Procedures should be based on the incident response policy. Standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team. SOPs should be comprehensive and detailed to ensure that the priorities of the organization are reflected in the response operation. In addition, following standardized responses should minimize errors, particularly those that might be caused by incident handling tempo and stress. SOPs should be tested to validate accuracy and usefulness, and then distributed to all team members. Training should be provided for SOP users; the SOP documents can be used as an instructional tool.

Sharing Information with Outside Parties

The organization may need to communicate with outside parties regarding an incident. Incident handlers may also need to discuss the incident with other involved parties, such as the organization's Internet service provider (ISP), the ISP that the attacker is using, the vendor of vulnerable software, or other incident response teams that may be familiar with unusual activity that the handler is trying to understand. An organization may want to—or be required to—communicate incident details with an outside organization for numerous reasons. The incident response team should discuss this at length with the organization's public affairs office, legal department, and management before an incident occurs to establish policies and procedures regarding information sharing. Otherwise, sensitive information regarding incidents may be provided to unauthorized parties; this action could lead to greater disruption and financial loss than the incident itself. The team should document all contacts and communications with outside parties for liability and evidentiary purposes.

The following sections provide guidance on communicating with several types of outside parties regarding the handling of actual incidents, including the media, law enforcement, and incident reporting organizations. Figure 2 shows several outside parties with which the organization may need to communicate. The arrows indicate the direction of the communication—for example the organization may initiate communications with software vendors. Double-headed arrows indicate either party may initiate communications. Some of these outside parties are described below.

The Media

Dealing with the media is an important part of incident response. The incident handling team should establish media communications procedures that are in compliance with the organization's policies on appropriate interaction with the media and information disclosure. Organizations often find it beneficial to designate a single media point of contact (POC) and at least one backup contact for discussing incidents with

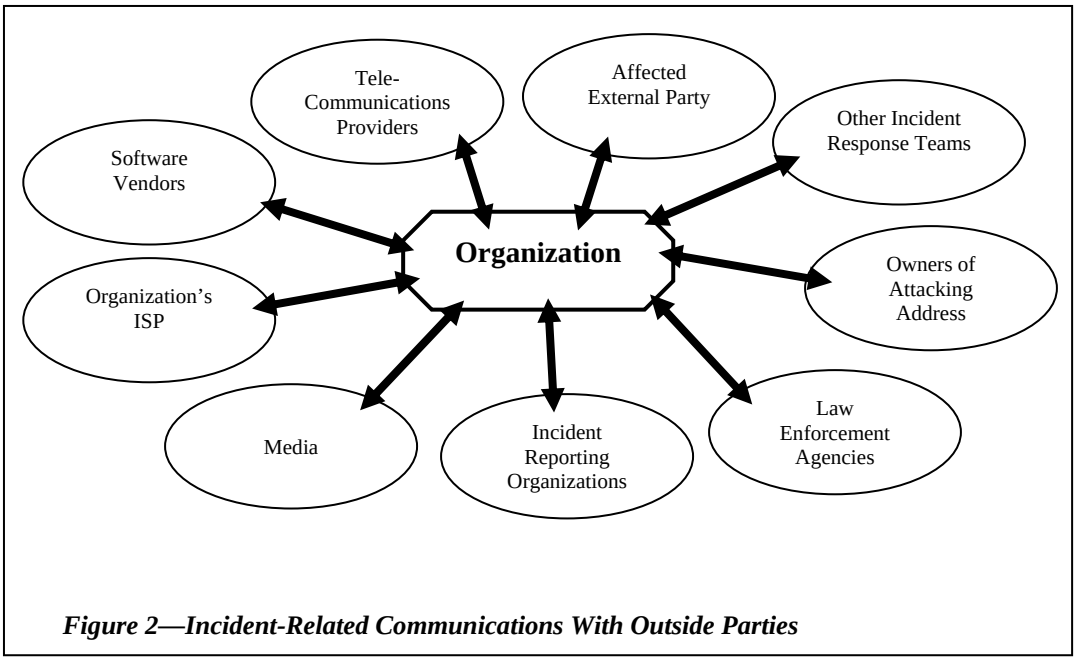

Figure 2—Incident-Related Communications With Outside Parties

the media. Ideally, all members of the incident response team should be prepared to interact with the media:

- Conduct training sessions on interacting with the media regarding incidents, which should include:
  - The importance of not revealing sensitive information, such as technical details of countermeasures (e.g., which protocols the firewall permits), which could assist other would-be attackers
  - The positive aspects of communicating important information to the public fully and effectively
- Establish procedures to brief media contacts on the issues and sensitivities regarding a particular incident before discussing it with the media.
- Hold mock interviews and press conferences during incident handling exercises. The following are examples of questions to ask the media contact:
  - Who attacked you?
  - When did it happen?
  - How did they do the attack?
  - How widespread is the incident?
  - Did this happen because you have poor security practices?
  - What steps are you taking to determine what happened?
  - What is the impact of this incident?
  - What is the estimated monetary cost of this incident?

Law Enforcement

One reason that many security-related incidents do not result in convictions is that organizations do not properly contact law enforcement. Several levels of law enforcement are available to investigate incidents: Federal investigatory agencies (e.g., in the United States the Federal Bureau of Investigation [FBI] and the U. S. Secret Service), district attorney offices, state law enforcement, and local (e.g., county) law enforcement. The incident response team should become acquainted with its various law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, and how it should be collected.

Law enforcement should be contacted through designed individuals in a manner consistent with the requirements of the law and the organization's procedures. Many organizations prefer to appoint one incident response team member as the primary POC with law enforcement. This person should be familiar with the reporting procedures for all relevant law enforcement agencies and well prepared to recommend which agency, if any, should be contacted. Note that the organization typically should not contact multiple agencies because doing so might result in jurisdictional conflicts. The incident response team should understand what the potential jurisdictional issues are (e.g., physical location—an organization based in one state has a server located in a second state attacked from a system in a third state, being used remotely by an attacker in a fourth state).

Incident Reporting Organizations

Organizations should create a policy that states who is designated to report incidents and how the incidents should be reported. Organizations may choose to report incidents to:

- **Information Analysis Infrastructure Protection (IAIP).** Because IAIP is part of the Department of Homeland Security (DHS), it is interested in any threats to critical U.S. infrastructures. Organizations can report incidents to IAIP using its incident report form.
- **CERT® Coordination Center (CERT®/CC).** CERT®/CC, previously known as CERT, is located at Carnegie Mellon University. This nongovernmental entity is interested in any computer security incidents involving the Internet. CERT®/CC provides an incident reporting system for online incident reporting.
- **The Organization's ISP.** During a network-based DOS attack, an organization may need assistance from its ISP in blocking the attack or tracing its origin.
- **Owners of Attacking Addresses.** If attacks are originating from an external organization's IP address space, incident handlers may want to talk to the designated security contacts for the organization to alert them to the activity or to ask them to collect evidence. Handlers should be cautious if they are unfamiliar with the external organization because the owner of the address space could be the attacker or an associate of the attacker.
- **Software Vendors.** Under some circumstances, incident handlers may want to speak to a software vendor about suspicious activity. This contact could include questions regarding the significance of certain log entries or known false positives for certain intrusion detection signatures, where minimal information regarding the incident may need to be revealed. More information may need to be provided in some cases—for example, if a server appears to have been compromised through an unknown software vulnerability. Incident handlers may have other questions for vendors, such as the availability of patches or fixes for new vulnerabilities.
- **Other Incident Response Teams.** An organization may experience an unusual incident that is similar to ones handled by other teams; sharing information can facilitate more effective and efficient incident handling for all teams involved. An alternative to joining a formal group is to participate in incident-related mailing lists, anonymously providing nonsensitive information on an incident and asking for opinions.
- **Affected External Parties.** An incident may affect external parties directly; for example, an outside organization may contact the agency and claim that one of the agency's users is attacking it. Another way in which external parties may be affected is if an attacker gains access to sensitive information regarding them, such as credit card information. In some jurisdictions, organizations are required to notify all parties that are affected by such an incident. Regardless of the circumstances, it is preferable for the organization to notify affected external parties of an incident before the media or other external organizations do so. Handlers should be careful to give out only appropriate information—the affected parties may request details about internal investigations that should not be revealed publicly.

It is highly recommended that the incident response team discuss with its public affairs office and legal department the circumstances under which each type of external organization can be contacted and the kind of information that can be provided. These procedures should be written, and all incident response team members should follow them.

Step 3: Organize a Security Incident Response Team

An incident response team should be available for contact by anyone who discovers or suspects that an incident involving the organization has occurred. One or more team members, depending on the magnitude of the incident and availability of personnel, will then handle the incident. The incident handlers analyze the incident data, determine the impact of the incident, and act appropriately to limit the damage to the

organization and restore normal services. Although the incident response team may have only a few members, the team's success depends on the participation and cooperation of individuals throughout the organization. This section identifies such individuals, discusses incident response team models, and provides guidance for selecting an appropriate model.

Incident response team structure models fall into one of three categories:

- **Central Incident Response Team.** A single incident response team handles incidents throughout the organization. This model is effective for small organizations and for large organizations with minimal geographic diversity in terms of computing resources.
- **Distributed Incident Response Teams.** The organization has multiple incident response teams, each responsible for handling incidents for a particular logical or physical segment of the organization. This model is effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant locations (e.g., one team per geographic region, one team per major facility). However, the teams should be part of a single centralized entity so that the incident response process is consistent across the organization and information is shared among teams. This is particularly important because multiple teams may see components of the same incident or may handle similar incidents. Strong communication among teams and consistent practices should make incident handling more effective and efficient.
- **Coordinating Team.** An incident response team provides guidance and advice to other teams without having authority over those teams—for example, a department-wide team may assist individual agencies' teams.

Incident response teams can also use any of three staffing models:

- **Employees.** The organization performs all of its incident response work, with limited technical and administrative support from contractors.
- **Partially Outsourced.** The organization outsources portions of its incident response work. although incident response duties can be divided among the organization and one or more outsourcers in many ways, a few arrangements have become commonplace:
  - Some organizations perform basic incident response work in-house and call on contractors to assist with handling incidents, particularly those that are more serious or widespread. The services most often performed by the contractors are computer forensics, advanced incident analysis, incident containment and eradication, and vulnerability mitigation.
- **Fully Outsourced.** The organization completely outsources its incident response work, typically to an onsite contractor. This model is most likely to be used when the organization needs a full-time, onsite incident response team but does not have enough available, qualified employees.
  - The most prevalent arrangement is for the organization to outsource 24-hour-a-day, 7-day-a-week (24/7) monitoring of intrusion detection sensors, firewalls, and other security devices to an offsite managed security services provided (MSSP). The MSSP identifies and analyzes suspicious activity and reports each detected incident to the organization's incident response team. Because the MSSP employees can monitor activity for multiple customers simultaneously, this model may provide a 24/7 monitoring and response capability at a skill and cost level that is superior to a comparable internal team.

Team Model Selection

When selecting appropriate structure and staffing models for an incident response team, organizations should consider the following factors:

- **The Need for 24/7 Availability.** Larger organizations, as well as smaller ones that support critical infrastructures, usually need incident response staff to be available 24/7. This typically means that incident handlers can be contacted at any time by phone or

pager, but it can also mean that an onsite presence is required at all times. Real-time availability is the best for incident response because the longer an incident lasts, the more potential there is for damage and loss. Real-time contact is often needed when working with other agencies and organizations—for example, tracing spoofed traffic back to its source through router hops. An incident response team that can react quickly to investigate, contain, and mitigate incidents should be genuinely useful to the organization.

- **Full-Time Versus Part-Time Team Members.** Organizations with limited funding, staffing, or incident response needs may have only part-time incident response team members. In this case, the incident response team can be thought of as a volunteer fire department. When an emergency occurs, the team members are contacted rapidly, and those who can assist do so. An existing group such as the IT help desk can act as a first POC for incident reporting. The help desk members can be trained to perform the initial investigation and data gathering and then alert the incident response team if it appears that a serious incident has occurred. Organizations with part-time team members should ensure that they maintain their incident response skills and knowledge.
- **Employee Morale.** Incident response work is very stressful, as are the on-call responsibilities of most team members. This combination makes it easy for incident response team members to become overly stressed. Many organizations will also struggle to find willing, available, experienced, and properly skill people to participate, particularly in 24-hour support.
- **Cost.** Cost is a major factor, especially if employees are required to be onsite 24/7. Organizations may fail to include incident response-specific costs in budgets. For example, most organizations do not allocate sufficient funding for training and maintaining skills. Because incident response team works with many facets of IT, its members need much broader knowledge than most IT staff members. they must also understand how to use the tools of incident response, such as computer forensics software. The organization should also provide funding for regular team exercises so the team can gain practical experience and improve its performance. Other costs that may be overlooked are physical security for the team's work areas and communications mechanisms.
- **Staff Expertise.** Incident handling requires specialized knowledge and experience in several technical areas; the breadth and depth of knowledge required varies based on the severity of the organization's risks. Outsourcers may possess deeper knowledge of intrusion detection, vulnerabilities, exploits, and other aspects of security than employees of the organization. Also, managed security service providers may be able to correlate events among customers so that they can identify new threats more quickly than any individual customer could. However, technical staff members within the organization usually have much better knowledge of the organization's environment than an outsourcer would, which can be beneficial in identifying false positives associated with organization-specific behavior and the criticality of targets.
- **Organizational Structures.** If an organization has three departments that function independently, incident response may be more effective if each department has its own incident response team. The main organization can host a centralized incident response entity that facilitates standard practices and communications among the teams.

When considering outsourcing, organizations should keep these issues in mind:

- **Current and Future Quality of Work.** The quality of the outsourcer's work remains a very important consideration. Organizations should consider not only the current quality of work, but also the outsourcer's efforts to ensure the quality of future work—for example, minimizing turnover and burnout and providing a solid training program for new employees. Organizations should think about how they could audit or otherwise objectively assess the quality of the outsourcer's work.
- **Division of Responsibilities.** Organizations are usually unwilling to give an outsourcer

authority to make operational decisions for the environment (e.g., disconnecting a Web server). It is important to decide the point at which the outsourcer hands off the incident response to the organization. One partially outsourced model addresses this issue by having the outsourcer provide incident data to the organization's internal team, along with recommendations for further handling the incident. The internal team ultimately makes the operational decisions.

- **Sensitive Information Revealed to the Contractor.** Dividing incident response responsibilities and restricting access to sensitive information can limit this. For example, a contractor may determine what user ID was used in an incident but not know what person is associated with the user ID. The contractor can report to the organization that user ID 123456 is apparently being used to download pirated software without knowing who 123456 is. Trusted employees within the organization can then take over the investigation.
- **Lack of Organization-Specific Knowledge.** Accurate analysis and prioritization of incidents are dependent on specific knowledge of the organization's environment. The organization should provide the outsourcer regularly updated documents that define what incidents it is concerned about, which resources are critical, and what the level of response should be under various sets of circumstances. The organization also report all changes and updates made to its IT infrastructure, network configuration, and systems. Otherwise, the contractor has to make a best guess as to how each incident should be handled, inevitably leading to mishandled incidents and frustration on both sides. Lack of organization-specific knowledge can also be a problem when incident response is not outsourced, if communications are weak among teams or if the organization simply does not collect the necessary information.
- **Lack of Correlation.** Correlation among multiple data sources is very important. If the intrusion detection system records an attempted attack against a Web server, but the outsourcer has no access to the Web logs, it may be unable to determine whether the attack was successful. To be efficient, the outsourcer will require administrative privileges to critical systems and security device logs remotely over a secure channel. This will increase administration costs, introduce additional access entry points, and increase the risk of unauthorized disclosure of sensitive information.
- **Handling Incidents at Multiple Locations.** Effective incident response work often requires a physical presence at the organization's facilities. If the outsourcer is offsite, consider where the outsourcer is located, how quickly it can have an incident response team at any facility, and how much this will cost. Consider onsite visits; perhaps there are certain facilities or areas where the outsourcer should not be permitted to work.
- **Maintaining Incident Response Skills In House.** Organizations that completely outsource incident response should strive to maintain basic incident response skills in house. Situations may arise in which the outsourcer is unavailable (e.g., a new worm attacks thousands of organizations simultaneously, or a natural disaster or national flight stoppage occurs). The organization should be prepared to perform its own incident handling if the outsourcer is unable to act. The organization's technical staff must also be able to understand the significance, technical implications, and impact of the outsourcer's recommendations.

Incident Response Personnel

Regardless of which incident response model an organization chooses, a single employee should be in charge of incident response. In a fully outsourced model, this person is responsible for overseeing and evaluating the outsourcer's work. In all other models, this responsibility is generally achieved by having a team manager and a deputy team manager who assumes authority in the absence of the team manager. The managers typically perform a variety of tasks, including acting as a liaison with upper management and other teams and organizations, defusing crisis situations, and ensuring that the team has the necessary personnel, resources, and skills. Managers should also be technically adept and have excellent

communication skills, particularly in ability to communicate to a range of audiences. Finally, team managers should be able to maintain positive working relationships with other groups, even under times of high pressure.

In addition to the team manger and deputy team manager, some teams also have a technical lead—a person with strong technical skills and incident response experience who assumes oversight of and final responsibility for the quality of the technical work that the entire incident response team undertakes. The position of technical lead should not be confused with the position of incident lead. Larger teams often assign an incident lead as the primary POC for handling a specific incident. Depending on the size of the incident response team and the magnitude of the incident, the incident lead may not actually perform any actual incident handling, such as data analysis or evidence acquisition. Instead, the incident lead may be coordinating the handlers' activities, gathering information from the handlers, providing updates regarding the incident to other groups, and ensuring that the team's needs are met, such as arranging for food and lodging for the team during extended incidents.

Members of the incident response team should have excellent technical skills because they are critical to the team's success. Unless the team members command a high level of technical respect across the organization, people will not turn to them for assistance. Technical inaccuracy in functions such as issuing advisories can undermine the team's credibility, and poor technical judgment can cause incidents to worsen. Critical technical skills include system administration, network administration, programming, technical support, and intrusion detection. Every team member should have good problem solving skills; there is no substitute for real-world troubleshooting experience, such as dealing with operational outages. If it not necessary for every team member to be a technical expert—to large degree, practical and funding considerations will dictate this—but having at least one highly proficient person in each major area of technology (e.g., particular operating systems, Web servers, and email servers) is a necessity.

It is important to counteract staff burnout by providing opportunities for learning and growth. Suggestions for building and maintaining skills are as follows:

- Budget enough funding to maintain, enhance, and expand proficiency in technical areas and security disciplines, as well as less technical topics such as the legal aspects of incident response.
- Ensure the availability of books, magazines, and other technical references that promote deeper technical knowledge.
- Give team members opportunities to perform other tasks, such as creating educational materials, conducting security awareness workshops, writing software tools to assist system administrators in detecting incidents, and conducting research.
- Consider rotating staffing so that team members can have uninterrupted time off (e.g., vacations).
- Maintain sufficient staffing so that team members temporarily trade places with others (e.g., network administrators) to gain new technical skills.
- Occasionally bring in outside experts (e.g., contractors) with deep technical knowledge in needed areas, as funding permits.
- Develop incident handling scenarios and have the team members discuss how they would handle them.
- Conduct simulated incident handling exercises for the team. Exercises are particularly important because they not only improve the performance of the incident handlers, but also identify issues with policies and procedures, and with communication.

Incident response team members should have other skills in addition to technical expertise. Teamwork skills are fundamental importance because cooperation and coordination are necessary for successful incident response. Every team member should also have good communication skills. Speaking skills are particularly important because the team will interact with a wide variety of people, including incident victims, managers, system administrators, human resources, public affairs, and law enforcement. Writing skills are important when team members are preparing advisories and procedures. Although not everyone

within a team needs to have strong writing and speaking skills, at least a few people within every team should possess them so the team can represent itself well in front of senior management, users, and the public at large.

Dependencies Within Organizations

It is important to identify other groups within the organization that may be needed to participate in incident handling so that their cooperation can be solicited before it is needed. Every incident response team relies on the expertise, judgment, and abilities of others, including:

- **Management.** Management invariably plays a pivotal role in incident response. In the most fundamental sense, management establishes incident response policy, budget, and staffing. Ultimately, management is held responsible for coordinating incident response among various stakeholders, minimizing damage, and reporting to other parties. Without management support, an incident response team is unlikely to be successful.
- **Information Security.** Members of the information security team are often the first to recognize that an incident has occurred or is occurring and may perform the initial analysis of incidents. In addition, information security staff members may be needed during other stages of incident handling—for example, altering network security controls (e.g., firewall rulesets) to contain an incident.
- **Telecommunications.** Some incidents involve unauthorized access to telephone lines, such as dialing into unsecured modems. Private Branch Exchange (PBX) compromises often are intertwined with break-ins into other systems. The telecommunications staff is aware of the current capabilities and the POCs and procedures for working with telecommunications carriers.
- **IT Support.** IT technical experts (e.g., system administrators, network administrators, and software developers) not only have the needed technical skills to assist during an incident but also usually have the best understanding of the technology with which they deal on a daily basis. This understanding can facilitate decisions such as whether to disconnect an attacked system from the network.
- **Legal Department.** Legal experts should review incident response policies and procedures to ensure their compliance with law and Federal guidance, including the right to privacy. In addition, the guidance of the general counsel or legal department should be sought if there is reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect or a lawsuit.
- **Public Affair and Media Relations.** Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public (within the constraints imposed by security and law enforcement interests).
- **Human Resources.** When an employee is the apparent target of an incident or is suspected of causing an incident, the human resources department often becomes involved—for example, in assisting with disciplinary proceedings or employee counseling.
- **Business Continuity Planning.** Computer security incidents undermine the business resilience of an organization and act as a barometer of its level of vulnerabilities and the inherent risks. Business continuity planning professionals should be made aware of incidents and their impacts so they can fine-tune business impact assessments, risk assessments, and continuity and operations plans. Further, because business continuity planners have extensive expertise in minimizing operational disruption during severe circumstances, they may be valuable in planning responses to certain types of incidents, such as a denial of service (DOS). Organizations should also ensure that incident response policies and

procedures and business continuity processes are in sync.

- **Physical Security and Facilities Management.** Some computer security incidents occur through breaches of physical security or involve coordinated logical and physical attacks. Threats made against the organization may not indicate whether logical or physical resources are being targeted. The incident response team also may need access to facilities during incident handling—for example, to acquire a compromised workstation from a locked office. Thus, close coordination between physical security and facilities management and the incident response team is important.

Step 4: Assign Team Other Security Incident Response Responsibilities (as appropriate)

The main focus of an incident response team is performing incident response; however, it is fairly rare for a team to perform incident response only. The following are examples of additional services that an incident response team might offer.

- **Advisory Distribution.** A team may issue advisories that describe new vulnerabilities in operating systems and applications and provide information on mitigating the vulnerabilities. Promptly releasing such information is a high priority because of the direct link between vulnerabilities and incidents. Distributing information about current incidents also can be useful in helping others identify signs of such incidents. It is recommended that only a single team within the organization distribute computer security advisories, to avoid duplication of effort and the spread of conflicting information.
- **Vulnerability Assessment.** An incident response team can examine networks, systems, and applications for security-related vulnerabilities, determine how they can be exploited and what the risks are, and recommend how the risks can be mitigated. These responsibilities can be extended so that the team performs auditing or penetration testing, perhaps visiting sites unannounced to perform on-the-spot assessments. Incident handlers are well suited to performing vulnerability assessments because they routinely see all kinds of incidents and have first-hand knowledge of vulnerabilities and how they are exploited. However, because the availability of incident handlers is unpredictable, organizations should typically give primary responsibility for vulnerability assessments to another team and use incident handlers as a supplemental resource.
- **Intrusion Detection.** An incident response team may assume responsibility for intrusion detection because others within the organization do not have sufficient time, resources, or expertise. The team generally benefits because it should be poised to analyze incidents more quickly and accurately, based on the knowledge it gains of intrusion detection technologies. Ideally, however, primary responsibility for intrusion detection should be assigned to another team, with members of the incident response team participating in intrusion detection as their availability permits.
- **Education and Awareness.** Education and awareness are resource multipliers—the more the users and technical staff know about detecting, reporting, and responding to incidents, the less drain there should be on the incident response team. This information can be communicated through many means: workshops and seminars, Web sites, newsletters, posters, and even stickers on monitors.
- **Technology Watch.** A team can perform a technology watch function, which means that it looks for new trends in information security threats. Examples of this are monitoring security-related mailing lists, analyzing intrusion detection data to identify an increase in worm activity, researching new rootkits that are publicly available, and monitoring honeypots. The team should then make recommendations for improving security controls based on the trends that they identify. A team that performs a technology watch function should also be better prepared to handle new types of incidents.
- **Patch Management.** giving the incident response team the responsibility for patch

management (e.g., acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization) is generally not recommended. Patch management is a time-intensive, challenging task that cannot be delayed every time an incident needs to be handled. In fact, patch management services are often needed most when attempting to contain, eradicate, and recover from large-scale incidents. Effective communication channels between the patch management staff and the incident response team are likely to improve the success of a patch management program.

CHECK PROCEDURES

The individuals responsible for developing this practice need to exercise quality control procedures to ensure that the practice has been implemented as specified. A quality control checklist (see Workpaper #1) is designed to assist in this process. At the conclusion of the four-step process the questions on

Workpaper #1 should be responded to in the following manner: If the team believes that they have correctly followed the practice as specified in this document, they should respond yes. If the team has overlooked a specific step, does not believe that they have followed it correctly, they should respond no. All no responses should be investigated and resolved.

USAGE TIPS

Usage tips to help improve the effectiveness of the security response team are summarized below.

- **Establish a formal incident response capability.** Organizations should be prepared to respond quickly and effectively when computer security defenses are breached.
- **Create an incident response policy and use it as the basis for incident response procedures.** The incident response policy is the foundation of the incident response program. It defines which events are considered incidents, establishes the organizational structure for incident response, defines roles and responsibilities, and lists the requirements for reporting incidents, among other items.
- **Establish policies and procedures regarding incident-related information sharing.** The organization will want or be required to communicate incident details with outside parties, such as the media, law enforcement agencies, and incident reporting organizations. The incident response team should discuss this requirement at length with the organization's public affairs office, legal department, and management to establish policies and procedures regarding information sharing. The team should comply with existing organization policy on interacting with the media and other outside parties.
- **Provide pertinent information on incidents to the appropriate incident reporting organization.** Organizations can contact other incident reporting organizations. Reporting is beneficial because the incident reporting organizations use the reported data to provide information to the reporting parties regarding new threats and incident trends.
- **Consider the relevant factors when selecting an incident response team model.** Organizations should carefully weigh the advantages and disadvantages of each possible team structure model and staffing model in the context of the organization's needs and available resources.
- **Select people with appropriate skills for the incident response team.** The credibility and proficiency of the team depend to a large extent on the technical skills of its members. Poor technical judgment can undermine the team's credibility and cause incidents to worsen. Critical technical skills include system administration, network administration, programming, technical support, and intrusion detection. Teamwork and communication skills are also needed for effective incident handling.
- **Identify other groups within the organization that may need to participate in incident handling.** Every incident response team relies on the expertise, judgment, and abilities of other teams, including management, information security, IT support, legal, public affairs, and facilities management.

Determine which services the team should offer. Although the main focus of the team is incident response, most teams perform additional functions. Examples include the distributing security advisories, performing vulnerability assessments, educating users on security and monitoring intrusion detection sensors.

DELIVERABLES

The primary deliverable from this practice is an established security incident response practice. This means that there is a formalized method for handling security incidents and that a team will be established to make that response in that formal manner. Included within this deliverable are two sub-deliverables which are the team that will respond to incidents and management's policy on incident reporting.

Workpaper #1 – Quality Control Checklist for Organizing a Computer Security Incident Response Capability

	ITEM	**RESPONSE (Circle One)**		**COMMENTS**
1.	Has a security event been defined?	**Yes**	**No**	
2.	Has a security incident been defined?	**Yes**	**No**	
3.	Has the organization recognized the need for a formal incident response?	**Yes**	**No**	
4.	If so, is the organization willing to expend resources to formalize an incident response?	**Yes**	**No**	
5.	If so, is the organization willing to organize a security response team?	**Yes**	**No**	
6.	Has management defined an incident response policy?	**Yes**	**No**	
7.	If so, does this policy identify the purpose and objective for the security response effort?	**Yes**	**No**	
8.	Has the organization identified who they will share incident response information with?	**Yes**	**No**	
9.	If so, have they made contact with that organization to develop a relationship for reporting incident responses and receiving information back?	**Yes**	**No**	
10.	Does the organization that they will share information with include the media?	**Yes**	**No**	
11.	Does the organization that they will share information with include the software vendors?	**Yes**	**No**	
12.	Does the organization that they will share information with include the telecommunication providers?	**Yes**	**No**	
13.	Does the organization that they will share information with include the effected external parties?	**Yes**	**No**	
14.	Does the organization that they will share information with include the other incident response teams?	**Yes**	**No**	
15.	Does the organization that they will share information with include the law enforcement agencies?	**Yes**	**No**	
16.	Does the organization that they will share information with include the owners of attacking addresses?	**Yes**	**No**	
17.	Does the organization that they will share information with include the incident reporting organizations?	**Yes**	**No**	
18.	Do the organizers of the incident response team understand the three categories of team models?	**Yes**	**No**	
19.	If so, have they selected an appropriate model for incident reporting?	**Yes**	**No**	
20.	Has the team organizing effort identified the skills required on the incident response team?	**Yes**	**No**	
21.	If so, do they individuals assigned to the team have those skills?	**Yes**	**No**	

22.	Have the incident response team organizers identified other responsibilities that the team might undertake?	**Yes**	**No**	
23.	If so, has the team been assigned the appropriate responsibilities for the organization?	**Yes**	**No**	