# CHAPTER 2

# Introduction to the Incident Response Process

In our experience, we have responded to the gamut of incidents: criminal incidents, incidents that involved civil litigation, and incidents that disrupted business but were not actionable (cases where criminal or civil action was improbable). We also have developed incident response plans for numerous organizations, ranging from financial services institutions to companies that produce mainstream products. During our various responses and program development engagements, we sought to design an incident response process that will work with each type of incident you may encounter. We believe that the incident response process we introduce in this chapter meets the needs of any organization or individual who must respond to computer security incidents. We also believe that law enforcement or hired investigators should understand all of the phases of this methodology, even if they perform actions during only a portion of the entire process.

Before we delve into the specifics of the incident response methodology, we need to answer some basic questions about incident response: What do we mean by a computer security incident? What are the goals of incident response? Who is involved in the incident response process?

## WHAT IS A COMPUTER SECURITY INCIDENT?

We define a *computer security incident* as any unlawful, unauthorized, or unacceptable action that involves a computer system or a computer network. Such an action can include any of the following events:

- Theft of trade secrets
- Email spam or harassment
- Unauthorized or unlawful intrusions into computing systems
- Embezzlement
- Possession or dissemination of child pornography
- Denial-of-service (DoS) attacks
- Tortious interference of business relations
- Extortion
- Any unlawful action when the evidence of such action may be stored on computer media such as fraud, threats, and traditional crimes.

Notice that many of these events include violations of public law, and they may be actionable in criminal or civil proceedings. Several of these events have a grave impact on an organization's reputation and its business operations. Responding to computer security incidents can involve intense pressure, time, and resource constraints.

A severe incident affecting critical resources can seem overwhelming. Furthermore, no two incidents are identical, and very few will be handled in exactly the same manner.

However, breaking down the procedure into logical steps makes incident response manageable. In this chapter, we introduce an effective methodology that will provide your organization with a tested and successful approach to resolving computer security incidents.

## WHAT ARE THE GOALS OF INCIDENT RESPONSE?

In our incident response methodology, we emphasize the goals of corporate security professionals with legitimate business concerns, but we also take into consideration the concerns of law enforcement officials. Thus, we developed a methodology that promotes a coordinated, cohesive response and achieves the following:

- ▼ Prevents a disjointed, noncohesive response (which could be disastrous)
- ■ Confirms or dispels whether an incident occurred
- ■ Promotes accumulation of accurate information
- ■ Establishes controls for proper retrieval and handling of evidence
- ■ Protects privacy rights established by law and policy
- ■ Minimizes disruption to business and network operations
- ■ Allows for criminal or civil action against perpetrators
- ■ Provides accurate reports and useful recommendations
- ■ Provides rapid detection and containment
- ■ Minimizes exposure and compromise of proprietary data
- ■ Protects your organization's reputation and assets
- ■ Educates senior management
- ▲ Promotes rapid detection and/or prevention of such incidents in the future (via lessons learned, policy changes, and so on)

## WHO IS INVOLVED IN THE INCIDENT RESPONSE PROCESS?

Incident response is a multifaceted discipline. It demands a myriad of capabilities that usually require resources from several different operational units of an organization. Human resources personnel, legal counsel, technical experts, security professionals, corporate security officers, business managers, end users, help desk workers, and other employees may find themselves involved in responding to a computer security incident.

Most organizations establish a team of individuals, often referred to as a *Computer Security Incident Response Team* (*CSIRT*), to respond to any computer security incident. The CSIRT is a multidisciplined team with the appropriate legal, technical, and other

### The Role of the Corporate Computer Security Incident Response Team

There is often a rift between personnel who investigate computer security incidents and those who investigate traditional crimes. Many corporations delineate separate functions for corporate security personnel and computer security personnel. The CSIRT responds only to network attacks such as computer intrusions or DoS attacks. When a more traditional crime is committed, corporate security officers or corporate investigators perform the investigation. However, it is very common for the corporate security personnel to be unarmed and unprepared to deal with technical evidence. This same technical evidence is often trivial and simple for the CSIRT personnel to interpret.

Since members of your incident response team have the technical skills required to perform successful investigations that involve technical evidence, they could be employed to do so, regardless of the incident that created the technical evidence. In the future, we foresee less of a divided field in corporate investigations. Everyone will need to obtain and understand technical evidence.

expertise necessary to resolve an incident. Since the CSIRT members have special expertise, and incident response is not required at all times, the CSIRT is normally a dynamic team assembled when an organization requires its capabilities.

## INCIDENT RESPONSE METHODOLOGY

We are always on a quest for the perfect way to organize a process. We search for the right way to define phases of the process, look for bright-line separation of phases to avoid murky areas, try to make the perfect flowchart to illustrate the process, and organize the phases so the process can be applied to the widest range of possible scenarios. Since the incident response process can involve so many variables and factors that affect its flow, it is quite a challenge to create a simple picture of the process while maintaining a useful level of accuracy. However, we feel that we have developed an incident response process that is both simple and accurate.

Computer security incidents are often complex, multifaceted problems. Just as with any complex engineering problem, we use a "black box" approach. We divide the larger problem of incident resolution into components and examine the inputs and outputs of each component. Figure 2-1 illustrates our approach to incident response. In our methodology, there are seven major components of incident response:

- **Pre-incident preparation** Take actions to prepare the organization and the CSIRT before an incident occurs.

- **Detection of incidents** Identify a potential computer security incident.
- **Initial response** Perform an initial investigation, recording the basic details surrounding the incident, assembling the incident response team, and notifying the individuals who need to know about the incident.
- **Formulate response strategy** Based on the results of all the known facts, determine the best response and obtain management approval. Determine what civil, criminal, administrative, or other actions are appropriate to take, based on the conclusions drawn from the investigation.
- **Investigate the incident** Perform a thorough collection of data. Review the data collected to determine what happened, when it happened, who did it, and how it can be prevented in the future.
- **Reporting** Accurately report information about the investigation in a manner useful to decision makers.
- **Resolution** Employ security measures and procedural changes, record lessons learned, and develop long-term fixes for any problems identified.

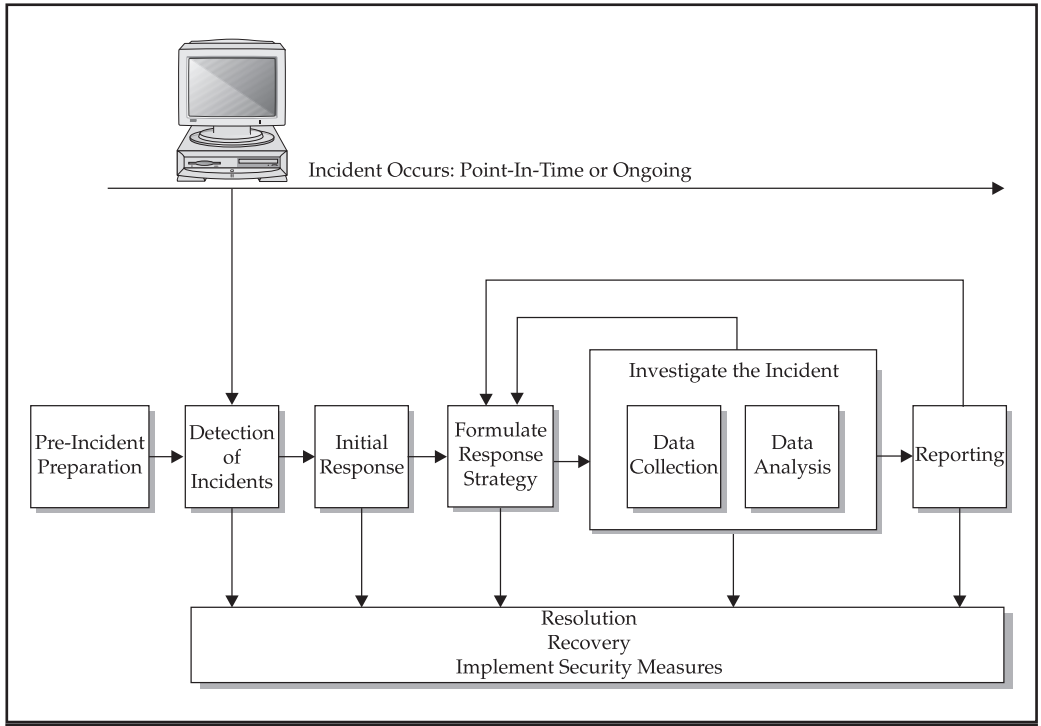


**Figure 2-1.** Seven components of incident response

We will discuss each of these steps in this chapter, focusing on the big picture. The remainder of this book focuses on achieving the goals of each step, with the greatest emphasis placed on the investigating the incident phase.

## Pre-Incident Preparation

Preparation leads to successful incident response. During this phase, your organization needs to prepare both the organization itself as a whole and the CSIRT members, *prior* to responding to a computer security incident.

We recognize that computer security incidents are beyond our control; as investigators, we have no idea when the next incident will occur. Furthermore, as investigators, we often have no control or access to the affected computers before an incident occurs. However, lack of control does not mean we should not attempt to posture an organization to promote a rapid and successful response to any incidents.

Incident response is reactive in nature. The pre-incident preparation phase comprises the *only* proactive measures the CSIRT can initiate to ensure that an organization's assets and information are protected.

Ideally, preparation will involve not just obtaining the tools and developing techniques to respond to incidents, but also taking actions on the systems and networks that will be part of any incident you need to investigate. If you are fortunate enough to have any level of control over the hosts and networks that you will be asked to investigate, there are a variety of steps you can take now to save time and effort later.

### Preparing the Organization

Preparing the organization involves developing all of the corporate-wide strategies you need to employ to better posture your organization for incident response. This includes the following:

- Implementing host-based security measures
- Implementing network-based security measures
- Training end users
- Employing an intrusion detection system (IDS)
- Creating strong access control
- Performing timely vulnerability assessments
- Ensuring backups are performed on a regular basis

### Preparing the CSIRT

The CSIRT is defined during the pre-incident preparation phase. Your organization will assemble a team of experts to handle any incidents that occur. Preparing the CSIRT includes considering at least the following:

- ▼ The hardware needed to investigate computer security incidents
- ■ The software needed to investigate computer security incidents
- ■ The documentation (forms and reports) needed to investigate computer security incidents
- ■ The appropriate policies and operating procedures to implement your response strategies
- ▲ The training your staff or employees require to perform incident response in a manner that promotes successful forensics, investigations, and remediation

You do not want to be acquiring essential resources *after* an incident occurs. Typically, you cannot afford unnecessary delays when attempting to resolve an incident.

Chapter 3 goes into detail about the hardware, software, documentation, policies, and training you need in place to prepare your organization and your CSIRT before an incident occurs.

## Detection of Incidents

If an organization cannot detect incidents effectively, it cannot succeed in responding to incidents. Therefore, the detection of incidents phase is one of the most important aspects of incident response. It is also one of the most decentralized phases, in which those with incident response expertise have the least control.

Suspected incidents may be detected in countless ways. Computer security incidents are normally identified when someone suspects that an unauthorized, unacceptable, or unlawful event has occurred involving an organization's computer networks or data-processing equipment. Initially, the incident may be reported by an end user, detected by a system administrator, identified by IDS alerts, or discovered by many other means. Some of the functional business areas involved in detection and some common indicators of a computer security incident are illustrated in Figure 2-2.

**NOTE** Organizations must have a well-documented and simple mechanism for reporting incidents. This is critical to establish accurate metrics, which is often required to obtain the proper budget required for an organization's incident response capability.

In most organizations, end users may report an incident through one of three avenues: their immediate supervisor, the corporate help desk (or local Information Technology department if there is no formal help desk), or an incident hotline managed by the Information Security entity. Typically, end users report technical issues to the help desk, while employee-related issues are reported to a supervisor or directly to the local Human Resources department.

No matter how you detect an incident, it is paramount to record all of the known details. We suggest using an initial response checklist to make sure you record the pertinent facts. The initial response checklist should account for many details, not all of which will

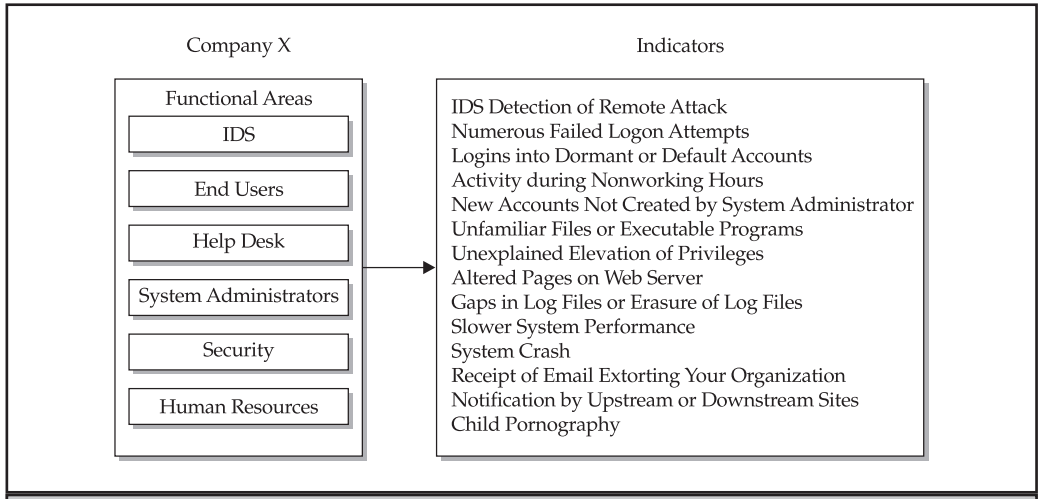


**Figure 2-2.** Detection of incidents

be readily discernable immediately after an incident is detected. Just record the known facts. Some of the critical details include the following:

- Current time and date
- Who/what reported the incident
- Nature of the incident
- When the incident occurred
- Hardware/software involved
- Points of contact for involved personnel

A more complete example of an initial response checklist is included in the appendix.

After completing the initial response checklist, the CSIRT should be activated and the appropriate people contacted. The CSIRT will use the information from the initial response checklist to begin the next phase of the response process, the initial response.

## Initial Response

One of the first steps of any investigation is to obtain enough information to determine an appropriate response. The initial response phase involves assembling the CSIRT, collecting network-based and other data, determining the type of incident that has occurred, and assessing the impact of the incident. The idea is to gather enough information to

## Eye Witness Report

Computer security incidents can be detected in countless ways. One of the largest economic espionage investigations the Department of Justice has conducted began with nontechnical indicators. An employee of a large telecommunications company witnessed another employee placing proprietary hardware into a gym bag. It was commonly accepted that employees at this company worked at home, and the programs they developed all worked on their specialized equipment. However, the witness noticed that this particular employee continued to "sneak" proprietary components out of the organization in a gym bag.

Rather than approach and alert the employee, the witness was prudent enough to report the incident to the appropriate people. The witness recognized that the pilfering of the hardware may be a symptom of something much more devastating: the theft of the company's prized source code. By not alerting the employee, the witness fostered excellent incident response. The organization was able to implement steps to collect additional evidence to determine whether the employee was also pilfering the source code.

begin the next phase, which is developing a response strategy. The other purpose of the initial response phase is to document steps that must be taken. This approach prevents "knee-jerk" reactions and panic when an incident is detected, allowing your organization to implement a methodical approach in the midst of a stressful situation.

The individuals involved with detecting an incident actually begin the initial response phase. The details surrounding the incident are documented by whoever detected the incident or by an individual who was notified that the incident may have occurred (for example, help desk or security personnel). The control of the response should be forwarded to the CSIRT early in the process to take advantage of the team's expertise; the more steps in the initial response phase performed by the CSIRT, the better.

Typically, the initial response will not involve touching the affected system(s). The data collected during this phase involves reviewing network-based and other evidence. This phase involves the following tasks:

- ▼ Interviewing system administrators who might have insight into the technical details of an incident
- ■ Interviewing business unit personnel who might have insight into business events that may provide a context for the incident
- ■ Reviewing intrusion detection reports and network-based logs to identify data that would support that an incident has occurred
- ▲ Reviewing the network topology and access control lists to determine if any avenues of attack can be ruled out

At a minimum, the team must verify that an incident has actually occurred, which systems are directly or indirectly affected, which users are involved, and the potential business impact. The team should verify enough information about the incident so that the actual response will be appropriate. It may be necessary to initiate network monitoring at this stage, simply to confirm an incident is occurring. The key here is determining how much information is enough before formulating your overall response strategy. The answer depends on many factors, which we address in detail in Chapter 4.

At the conclusion of the initial response stage, you will know whether or not an incident has occurred and have a good idea of the systems affected, the type of incident, and the potential business impact. Armed with this information, you are now ready to make a decision on how to handle the incident.

## Formulate a Response Strategy

The goal of the response strategy formulation phase is to determine the most appropriate response strategy, given the circumstances of the incident. The strategy should take into consideration the political, technical, legal, and business factors that surround the incident. The final solution depends on the objectives of the group or individual with responsibility for selecting the strategy.

### Considering the Totality of the Circumstances

Response strategies will vary based on the circumstances of the computer security incident. The following factors need to be considered when deciding how many resources are needed to investigate an incident, whether to create a forensic duplication of relevant systems, whether to make a criminal referral, whether to pursue civil litigation, and other aspects of your response strategy:

- How critical are the affected systems?
- How sensitive is the compromised or stolen information?
- Who are the potential perpetrators?
- Is the incident known to the public?
- What is the level of unauthorized access attained by the attacker?
- What is the apparent skill of the attacker?
- How much system and user downtime is involved?
- What is the overall dollar loss?

Incidents vary widely, from virus outbreaks to theft of customers' credit card information. A typical virus outbreak generally results in some downtime and lost productivity, while the theft of customers' credit card information could put a fledgling dot-com operation out of business. Accordingly, the response strategy for each event will differ. A virus outbreak is more likely to be swept under the rug; the theft of credit card information

is the equivalent of a five-alarm fire, forcing a response that involves the Public Relations department, the CEO, and all available technical resources.

Details obtained during the initial response can be critical when choosing a response strategy. For example, a DoS attack originating from a university may be handled much differently from how an equivalent DoS attack originating from a competitor is handled. Before the response strategy is chosen, it may become necessary to reinvestigate details of the incident.

Factors other than the details of the incident will contribute to the response strategy. Most notably, your organization's response posture plays a large role in your response strategy. Your *response posture* is your capacity to respond, determined by your technical resources, political considerations, legal constraints, and business objectives. For a detailed discussion of these factors, see Chapter 3.

## Considering Appropriate Responses

Armed with the circumstances of the attack and your capacity to respond, you should be able to arrive at a viable response strategy. Table 2-1 shows some common situations with response strategies and potential outcomes. As you can see, the response strategy determines how you get from an incident to an outcome.

**NOTE** Your response strategy may be significantly impacted by existing (or lack) of Internet use policies, monitoring policies, and previous enforcement of policies.

### Eye Witness Report

We responded to an incident at a financial services organization, where an external attacker had obtained access to a database containing client information. The attacker eventually sent an email message to the organization, requesting a fee in order to patch the compromised system. This email included a file attachment that contained more than 17,000 records, each with the client name, address, date of birth, mother's maiden name, and private bank account numbers. The investigation revealed that the intruder did not obtain access to credit card numbers or social security numbers; he had solely the information contained in the email's file attachment.

On the day the financial services organization received the extortion email, the managers felt inclined to notify their clients. At a minimum, they felt they could at least notify the 17,000 clients whose information had been compromised. However, after careful deliberation, the managers reversed their initial inclination. Their assessment of the "risks versus rewards" of disclosing the details of the incident to their clients concluded that the risk of damage to corporate reputation outweighed the threat of identity theft. The organization would not notify any of their clients. This complete reversal of their response strategy took place in under three hours.

| Incident | Example | Response Strategy | Likely Outcome |
|---|---|---|---|
| DoS attack | TFN DDoS attack (A Popular Distributed Denial of Service Attack) | Reconfigure router to minimize effect of the flooding. | Effects of attack mitigated by router countermeasures. Establishment of perperator's identity may require too many resources to be worthwhile investment. |
| Unauthorized use | Using work computers to surf pornography sites | Possible forensic duplication and investigation. Interview with suspect. | Perpetrator identified, and evidence collected for disciplinary action. Action taken may depend on employee's position, or past enforcement of company policy. |
| Vandalism | Defaced web site | Monitor web site. Repair web site. Investigate web site while it is online. Implement web site "refresher" program. | Web site restored to operational status. Decision to identify perpetrator may involve law enforcement. |
| Theft of information | Stolen credit card and customer information from company database | Make public affairs statement. Forensic duplication of relevant systems. Investigation of theft. Law enforcement contacted. | Detailed investigation initiated. Law enforcement participation possible. Civil complaint filed to recover potential damages. Systems potentially offline for some time. |
| Computer intrusion | Remote administrative access via attacks such as cmsd buffer overflow and Internet Information Services (IIS) attacks | Monitor activities of attacker. Isolate and contain scope of unauthorized access. Secure and recover systems. | Vulnerability leading to intrusion identified and corrected. Decision made whether to identify perpetrators. |

**Table 2-1.** Possible Responses

As we have mentioned, the response strategy must take into consideration your organization's business objectives. For this reason, and because of the potential impact to your organization, the response strategy should be approved by upper-level management. Since upper-level management and TCP/IP discussions are usually oil and water, the response strategy options should be quantified with pros and cons related to the following:

- Estimated dollar loss
- Network downtime and its impact to operations
- User downtime and its impact to operations
- Whether or not your organization is legally compelled to take certain actions (is your industry regulated?)
- Public disclosure of the incident and its impact to the organization's reputation/business
- Theft of intellectual property and its potential economic impact

## Taking Action

Occasionally, an organization will need to take action to discipline an employee or to respond to a malicious act by an outsider. When the incident warrants, this action can be initiated with a criminal referral, a civil complaint, or some administrative reprimand or privilege revocation.

**Legal Action** It is not uncommon to investigate a computer security incident that is *actionable*, or could lead to a lawsuit or court proceeding. The two potential legal choices are to file a civil complaint or to notify law enforcement. Law enforcement involvement will reduce the autonomy that your organization has in dealing with an incident, and careful deliberation should occur before you engage the appropriate authorities. In cases where your organization feels compelled to notify law enforcement, you may want to determine the amount of effort and resources you want to invest in the investigation before bringing in a law enforcement agency.

The following criteria should be considered when deciding whether to include law enforcement in the incident response:

- Does the damage/cost of the incident merit a criminal referral?
- Is it likely that civil or criminal action will achieve the outcome desired by your organization? (Can you recover damages or receive restitution from the offending party?)
- Has the cause of the incident been reasonably established? (Law enforcement officers are not computer security professionals.)
- Does your organization have proper documentation and an organized report that will be conducive to an effective investigation?

- Can tangible investigative leads be provided to law enforcement officials for them to act on?
- Does your organization know and have a working relationship (prior liaison) with local or federal law enforcement officers?
- Is your organization willing to risk public exposure?
- Does the past performance of the individual merit any legal action?
- How will law enforcement involvement impact business operations?

**CAUTION** Do not mistake law enforcement officials for computer security consultants. If you notify them solely because you cannot implement the technical steps to remedy an incident, it is highly unlikely they will spend any time and effort to help. Their job is to investigate an incident, not to implement or advise in security measures that would prevent further attacks and damage to your organization from a reoccurring incident.

Table 2-2 shows several common scenarios and some potential actions that may lead to law enforcement involvement.

**Administrative Action** Disciplining or terminating employees via administrative measures is currently more common than initiating civil or criminal actions. Some administrative actions that can be implemented to discipline internal employees include the following:

- Letter of reprimand
- Immediate dismissal
- Mandatory leave of absence for a specific length of time (paid or unpaid)
- Reassignment of job duties (diminished responsibility)
- Temporary reduction in pay to account for losses/damage
- Public/private apology for actions conducted
- Withdrawal of certain privileges, such as network or web access

## Investigate the Incident

The investigation phase involves determining the who, what, when, where, how, and why surrounding an incident. You will conduct your investigation, reviewing host-based evidence, network-based evidence, and evidence gathered via traditional, nontechnical investigative steps.

No matter how you conduct your investigation, you are responding to an incident caused by *people*. People cause these incidents by using *things* to destroy, steal, access, hide, attack, and hurt other things. As with any type of investigation, the key is to determine which things were harmed by which people. However, a computer crime incident

| Incident | Action |
|---|---|
| DoS attack | Contact upstream providers to attempt to identify the likely source of the DoS attack. If the source is identified, consider notifying law enforcement to pierce the anonymity of the attacker and/or terminate the action. Your organization may also seek the help of the source ISP by requesting a breach of "Terms of Service" of the ISP by the attacker. |
| External attacker | Identify an IP address as the likely source and consider using law enforcement to pierce the anonymity behind the IP address. |
| Possession of child pornography | Your organization may be required to notify law enforcement. U.S. law currently dictates that failure to notify may risk criminal liability. Contact legal counsel and Human Resources immediately. Control access to the material and prevent dissemination. |
| Possession or dissemination of pornography | This activity is not investigated by law enforcement. Contact legal counsel and Human Resources to protect the organization from civil liability. Ensure your Acceptable Use Policy discourages such activity by employees. |
| Harassing email | This activity is not investigated by law enforcement. Contact legal counsel and Human Resources to protect the organization from potential civil liability. |

**Table 2-2.** Possible Actions

adds complexity to this simple equation. Establishing the identity behind the people on a network is increasingly difficult.

Users are becoming more adept at using encryption, steganography, anonymous email accounts, fakemail, spoofed source IP addresses, spoofed MAC addresses, masquerading as other individuals, and other means to mask their true identity in "cyberspace." In fact, establishing the identity of an attacker who brought down your web site can be so time consuming that most companies may elect not to even try. Since establishing identity can be less of a concern to the victim than the *things* harmed or damaged, many organizations choose to focus solely on what was damaged, how it was damaged, and how to fix it.

A computer security investigation can be divided into two phases: data collection and forensic analysis. During the data collection phase, you gather all the relevant information needed to resolve the incident in a manner that meets your response strategy. In the forensic analysis phase, you examine all the data collected to determine the who, what, when, where, and how information relevant to the incident. Figure 2-3 illustrates the possible steps taken during the two phases of investigation.

## Data Collection

*Data collection* is the accumulation of facts and clues that should be considered during your forensic analysis. The data you collect forms the basis of your conclusions. If you do not collect all the necessary data, you may not be able to successfully comprehend how an incident occurred or appropriately resolve an incident. You must collect data before you can perform any investigation.

Data collection involves several unique forensic challenges:

- ▼ You must collect electronic data in a forensically sound manner.
- ■ You are often collecting more data than you can read in your lifetime (computer storage capacity continues to grow).
- ▲ You must handle the data you collect in a manner that protects its integrity (evidence handling).

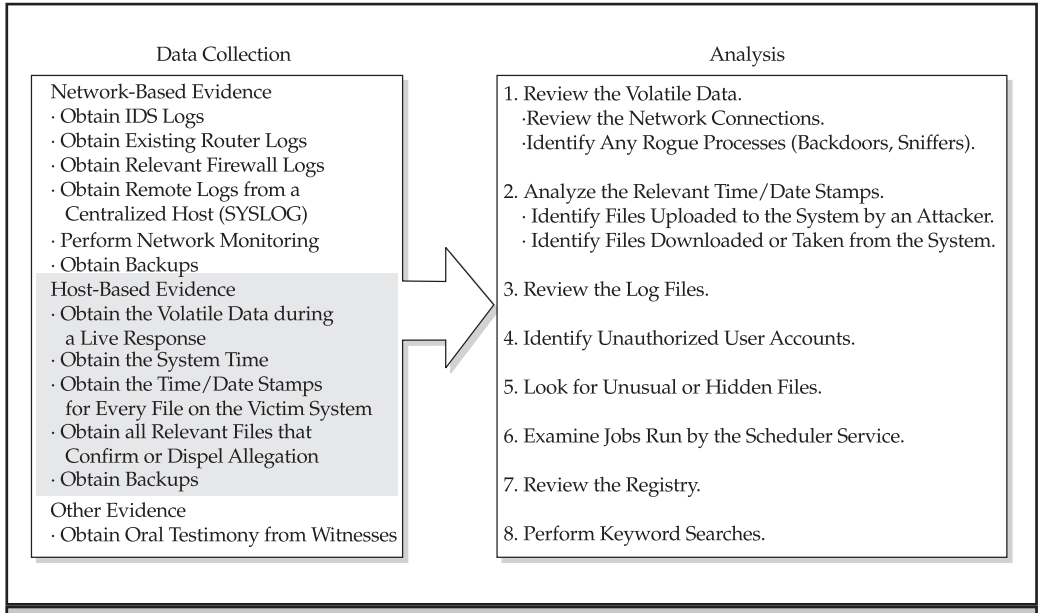


**Figure 2-3.** Possible investigation phase steps

These requirements show that special skills are required to obtain technical evidence. Chapters 5 through 9 of this book are devoted to proper data collection techniques, from gathering data from a live host to handling the evidence you've collected.

The information you obtain during the data collection phase can be divided into three fundamental areas: host-based information, network-based information, and other information.

**Host-based Information** Host-based evidence includes logs, records, documents, and any other information that is found on a system and not obtained from network-based nodes. For example, host-based information might be a system backup that harbors evidence at a specific period in time. Host-based data collection efforts should include gathering information in two different manners: *live data collection* and *forensic duplication*.

In some cases, the evidence that is required to understand an incident is ephemeral (temporary or fleeting) or lost when the victim/relevant system is powered down. This volatile data can provide critical information when attempting to understand the nature of an incident. Therefore, the first step of data collection is the collection of any volatile information from a host before this information is lost. The volatile data provides a "snapshot" of a system at the time you respond. You record the following volatile information:

- The system date and time
- The applications currently running on the system
- The currently established network connections
- The currently open sockets (ports)
- The applications listening on the open sockets
- The state of the network interface (promiscuous or not)

In order to collect this information, a *live response* must be performed. A live response is conducted when a computer system is still powered on and running. This means that the information contained in these areas must be collected without impacting the data on the compromised device. There are three variations of live response:

- **Initial live response** This involves obtaining only the volatile data from a target or victim system. An initial live response is usually performed when you have decided to conduct a forensic duplication of the media.
- **In-depth response** This goes beyond obtaining merely the volatile data. The CSIRT obtains enough additional information from the target/victim system to determine a valid response strategy. Nonvolatile information such as log files are collected to help understand the nature of the incident.
- **Full live response** This is a full investigation on a live system. All data for the investigation is collected from the live system, usually in lieu of performing a forensic duplication, which requires the system to be powered off.

Chapters 5 and 6 cover live data collection techniques, from Windows and Unix systems, respectively.

At some point (usually during your initial response), you need to decide whether or not to perform a forensic duplication of the evidence media. Generally, if the incident is severe or deleted material may need to be recovered, a forensic duplication is warranted. The forensic duplication of the target media provides the "mirror image" of the target system, which shows due diligence when handling critical incidents. It also provides a means to have working copies of the target media for analysis without worrying about altering or destroying potential evidence. If the intent is to take judicial action, law enforcement generally prefers forensic "bit-for-bit, byte-for-byte" duplicates of target systems. If the incident could evolve into a corporate-wide issue with grave consequences, it is prudent to perform a forensic duplication. Chapter 7 explains how to perform forensic duplication.

**Network-based Evidence** Network-based evidence includes information obtained from the following sources:

- IDS logs
- Consensual monitoring logs
- Nonconsensual wiretaps
- Pen-register/trap and traces
- Router logs
- Firewall logs
- Authentication servers

An organization often performs network surveillance (consensual monitoring) to confirm suspicions, accumulate evidence, and identify co-conspirators involved in an incident. Where host-based auditing may fail, network surveillance may fill in the gaps. Network surveillance is not intended to prevent attacks. Instead, it allows an organization to accomplish a number of tasks:

- Confirm or dispel suspicions surrounding an alleged computer security incident.
- Accumulate additional evidence and information.
- Verify the scope of a compromise.
- Identify additional parties involved.
- Determine a timeline of events occurring on the network.
- Ensure compliance with a desired activity.

Chapter 8 provides a detailed tutorial on how to collect and analyze network-based evidence.

**Other Evidence** The "other evidence" category involves testimony and other information obtained from people. This is the collection of evidence following more traditional investigative techniques. One can think of this as the collection of evidence via nontechnical means. This is when you collect personnel files, interview employees, interview witnesses, interview character witnesses, and document the information gathered.

## Forensic Analysis

*Forensic analysis* includes reviewing all the data collected. This includes reviewing log files, system configuration files, trust relationships, web browser history files, email messages and their attachments, installed applications, and graphic files. You perform software analysis, review time/date stamps, perform keyword searches, and take any other necessary investigative steps. Forensic analysis also includes performing more low-level tasks, such as looking through information that has been logically deleted from the system to determine if deleted files, slack space, or free space contain data fragments or entire files that may be useful to the investigation. Figure 2-4 depicts the major steps taken during forensic analysis.

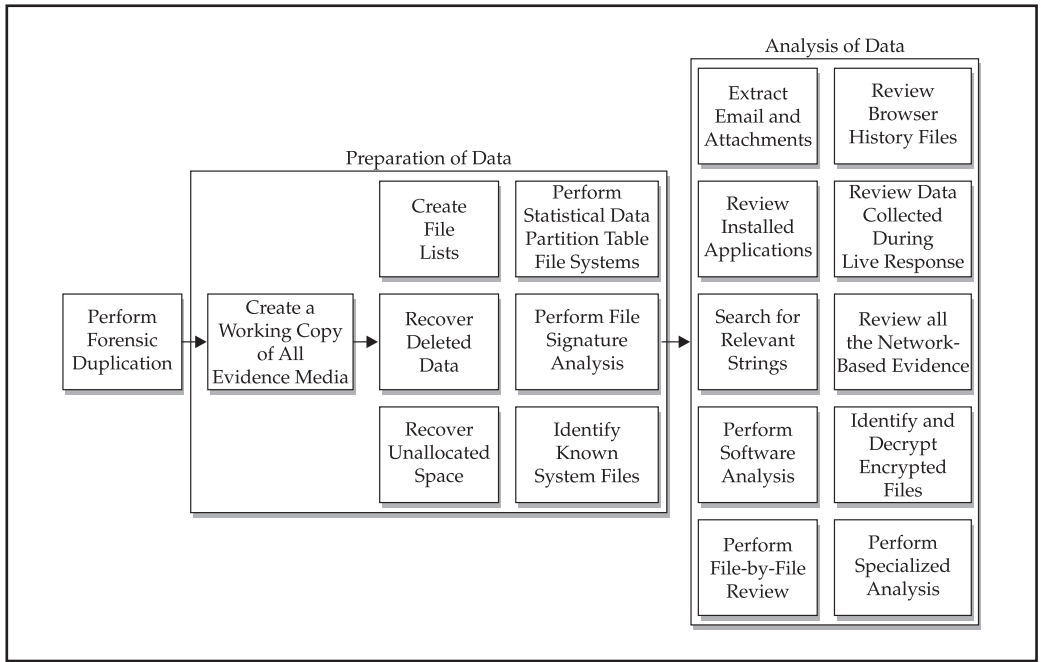


**Figure 2-4.** Performing forensic analysis

Forensic analysis requires that you perform some assembly and preparation of the data collected before you begin to analyze the data. Much of this process applies to the forensic analysis of host-based media, and in particular, hard drives. The preparation for analysis steps is discussed in depth in Chapter 10.

## Reporting

Reporting can be the most difficult phase of the incident response process. The challenge is to create reports that accurately describe the details of an incident, that are understandable to decision makers, that can withstand the barrage of legal scrutiny, and that are produced in a timely manner.

**NOTE** Reports are also often used by investigators to refresh their recollections during criminal trials and in training employees new to the field of computer forensics.

We have written thousands of pages of forensic reports in the past 12 months alone, and we have come up with some guidelines to ensure that the reporting phase does not become your CSIRT's nemesis:

- **Document immediately** All investigative steps and conclusions need to be documented as soon as possible. Writing something clearly and concisely at the moment you discover evidence saves time, promotes accuracy, and ensures that the details of the investigation can be communicated more clearly to others at any moment, which is critical if new personnel become involved or are assigned to lead the investigation.
- **Write concisely and clearly** Enforce the "write it tight" philosphy. Documenting investigative steps requires discipline and organization. Write everything down in a fashion that is understandable to you and others. Discourage shorthand or shortcuts. Vague notations, incomplete scribbling, and other unclear documentation can lead to redundant efforts, forced translation of notes, confirmation of notes, and a failure to comprehend notes made by yourself or others.
- **Use a standard format** Develop a format for your reports and stick to it. Create forms, outlines, and templates that organize the response process and foster the recording of all pertinent data. This makes report writing scalable, saves time, and promotes accuracy.

**CAUTION** We have seen "cut-and-paste" formatted reports that disclose other client's information by accident. We realize it is common sense to remove prior information when cutting and pasting information into reports, but, unfortunately, using templates can make a lazy person even lazier.

- **Use editors** Employ technical editors to read your forensic reports. This helps develop reports that are comprehensible to nontechnical personnel who have

an impact on your incident response strategy and resolution (such as Human Resources personnel, legal counsel, and business leaders). Unfortunately, editors can inadvertently change the meaning of critical information. The burden is still on you to review the final product prior to submission.

We provide additional details and examples of report writing in Chapter 17.

## Resolution

The goal of the resolution phase is to implement host-based, network-based, and procedural countermeasures to prevent an incident from causing further damage and to return your organization to a secure, healthy operational status. In other words, in this phase, you contain the problem, solve the problem, and take steps to prevent the problem from occurring again.

If you are accumulating evidence for potential civil, criminal, or administrative action, it is always a good idea to collect all evidence before you begin to implement any security measures that would alter the evidence obtained. If you rapidly secure a system by changing your network topology, implement packet filtering, or install software on a host without proper review and validation, good investigative clues—such as the state of the system at the time of the incident— are often lost!

The following steps are often taken to resolve a computer security incident:

1. Identify your organization's top priorities. Which of the following is the most critical to resolve: returning all systems to operational status, ensuring data integrity, containing the impact of the incident, collecting evidence, or avoiding public disclosure?
2. Determine the nature of the incident in enough detail to understand how the security occurred and what host-based and network-based remedies are required to address it.
3. Determine if there are underlying or systemic causes for the incident that need to be addressed (lack of standards, noncompliance with standards, and so on).
4. Restore any affected or compromised systems. You may need to rely on a prior version of the data, server platform software, or application software as needed to ensure that the system performs as you expect it to perform.
5. Apply corrections required to address any host-based vulnerabilities. Note that all fixes should be tested in a lab environment before being applied to production systems.
6. Apply network-based countermeasures such as access control lists, firewalls, or IDS.
7. Assign responsibility for correcting any systemic issues.
8. Track progress on all corrections that are required, especially if they will take significant time to complete.

9. Validate that all remedial steps or countermeasures are effective. In other words, verify that all the host-based, network-based, and systemic remedies have been applied correctly.
10. Update your security policy and procedures as needed to improve your response process.

## SO WHAT?

Understanding what a computer security incident is, what incident response means, and the steps taken during most responses puts your organization in a position to best protect its assets and its reputation. We have encountered all too often the company that seems incapable of handling even minor computer security incidents. As attacks become more crafty and more focused, your CIRT will need to be a well-oiled, capable (with the appropriate breadth of knowledge), well-mixed (including lawyers, technical staff, and perhaps law enforcement personnel), motivated team that fully understands the flow of incident response.

## QUESTIONS

1. What is the difference between *incident response* and *computer forensics*?
2. Which one of the following will a CSIRT not respond to?
   - Theft of intellectual property
   - Unauthorized access
   - SPAM
   - Extortion
   - Embezzlement
3. What are some of the advantages that an organized incident response program promotes?
4. What factors should be considered when deciding whether to include law enforcement in your incident response?
5. You arrive at work a few minutes early one day. As you walk past a few of the open employee cubicles, you notice several of the IT staff viewing inappropriate images on their monitors. You also notice that an employee seems offended and upset about it. Could this scenario lead to the formation of a computer security incident response team? What corporate entities (Human Resources, Public Affairs, etc.) would need to be involved in the response?
6. What is some of the volatile information you would retrieve from a computer system before powering it off?