**CHAPTER 1 RISK MANAGEMENT AND INCIDENT RESPONSE**

Information security is the art and practice of managing the confidentiality, integrity, and availability risks associated with in­formation. As you begin your exploration of the field, it is best to start with that in mind. In this chapter, we’ll explore the process that security professionals use to identify, assess, and manage the risks facing their organizations. We will also review the incident response procedures used when a risk materializes.

**OBJECTIVES IN THIS CHAPTER:**

Objective 1.1: Explain risk related concepts

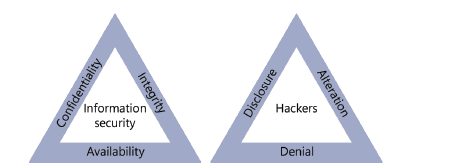
Objective 1.2: Carry out appropriate risk mitigation strategies

Objective 1.3: Execute appropriate incident response procedures

Objective 1.8: Exemplify the concepts of confidentiality, integrity and availability (CIA)

**CIA AND DAD TRIADS**

Security professionals, tasked with protecting the information assets of an organization, typi­cally think of their responsibilities in three realms: confidentiality, integrity, and availability (CIA). Adversaries, seeking to disrupt an organization’s security, have three corresponding goals in mind: disclosure, alteration, and denial (DAD). These models, shown in Figure 1-1, are known as the CIA and DAD triads and are the classic models embraced by security profession­als around the world.



**FIGURE 1-1 The CIA and DAD triads are the classic models of information security principles**.

**CONFIDENTIALITY AND DISCLOSURE**

The goal of confidentiality is to prevent unauthorized access to sensitive information. Quite simply, it is to keep secrets secret. Achieving confidentiality first requires that an organiza­tion classify its data, identifying which information assets are worthy of protection and the appropriate level of protection for each. For example, an organization might consider design documents for an unreleased product highly sensitive due to their competitive value. On the other hand, the internal phone book might be considerably less sensitive. Organizing confi­dential information into different data classifications allows security professionals to design appropriate controls, focusing scarce resources on the most sensitive data.

Adversaries, on the other hand, pursue the goal of disclosure, gaining access to sensitive information without permission. They may want to use this information for personal gain, to embarrass the organization publicly, or to simply make information freely available.

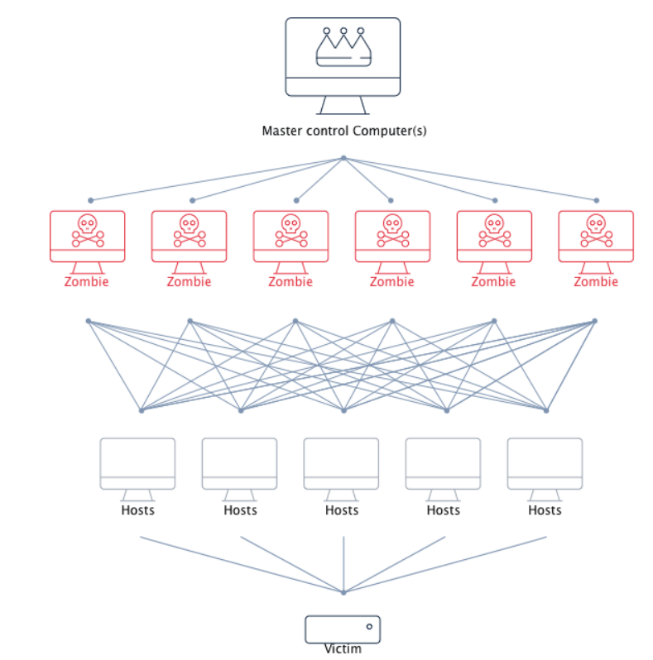
The WikiLeaks website, made famous by disclosures of sensitive US government information by Bradley Manning in 2010 and Edward Snowden in 2013, is dedicated to the disclosure of information that governments and corporations may find embarrassing.

**INTEGRITY AND ALTERATION**

Security professionals also pursue the goal of integrity, ensuring that information is only modified or deleted by authorized means. Protecting the integrity of information requires controls against deliberate alteration by adversaries such as an employee seeking to modify his payroll information without permission. It also requires protection against unintentional alteration, such as the corruption of data due to a software or hardware failure.

**AVAILABILITY AND DENIAL**

It’s not sufficient for security professionals to provide confidentiality and integrity con­trols.   
These must be supplemented with availability protection that ensures that authorized individuals have access to information when needed. Denial attacks occur when an adversary is able to successfully interrupt the availability of information, such as through a denial of ser­vice (DoS) attack. Adversaries might also attempt to harness many systems around the world to simultaneously perform a denial attack by using a technique known as distributed denial of service (DDoS).



**RISK ASSESSMENT AND MITIGATION**

In order to meet the three goals of confidentiality, integrity, and availability, security profes­sionals must have a solid understanding of the specific risks facing their organization. These will vary, depending upon the organization’s line of business, types of information handled, and even physical location. For example, an educational institution might consider the loss of student records, preventing grades from being issued, to be its greatest risk; whereas a military unit might believe that its greatest risk is the disclosure of secret plans that might lead to the death of personnel.

To perform an assessment of risks, we first must have a common language. There are three important terms related to risk assessment:

* Vulnerabilities Weaknesses in an organization’s security controls that might allow a breach of confidentiality, integrity, or availability. Vulnerabilities are internal factors.
* Threats External forces that might undermine the security controls of an organization.
* Risks Situations that occur when there is an intersection of a vulnerability in an organization’s security controls and a threat that seeks to exploit that vulnerability (see Figure 1-2).



**FIGURE 1-2 This equation shows the relationship between threats, vulnerabilities, and risks.**

*Consider the example of a web server that contains sensitive, password-protected informa­tion that has limited distribution to the customers of an organization. An individual who seeks to gain access to this information without paying is a threat to the confidentiality of that data.   
A misconfiguration in the web server that allows unlimited attempts to guess the password is a vulnerability. The combination of this vulnerability with a corresponding threat seeking to exploit it presents the risk that the organization’s information will be stolen.*

*A vulnerability without a corresponding threat does not pose a risk to the organization. For example, an organization’s data center might be vulnerable to flooding. If the data center is in a desert environment where there is no threat of flooding, there is no risk to manage. Simi­larly, a threat without a corresponding vulnerability also does not pose a risk. If an intruder knows how to pick locks, he may pose a threat to your organization, but if you use locks that have keypads rather than keys, they are not vulnerable to this threat. (Of course, they remain vulnerable to an intruder who knows how to defeat the keypad!)*

Organizations seeking to secure their information normally begin with a risk identification process that enumerates the threats facing the organization, the vulnerabilities in the organi­zation’s existing security controls, and the risks that result from intersections between these threats and vulnerabilities.

**LIKELIHOOD AND IMPACT (PROBABITE AND IMPACT)**

After an organization identifies those threats and vulnerabilities that pose a risk to their infor­mation assets, the next step in the risk assessment process is to evaluate the priority of those risks based upon two factors:

The likelihood that a risk will materialize. Some risks are simply more likely than others, depending upon the nature of the vulnerability or threat. For example, the threat of a physical break-in is much more likely to occur in a high-crime urban environment than it is on a military base located in a desert.

The impact that a risk will have on the organization if it does materialize. Some breaches of confidentiality, integrity, or availability will have more disruptive impacts on an or­ganization than others. For example, a successful website denial of service attack might have low impact on a construction firm, but the same attack would be disastrous for an e-commerce retailer that depends upon the website to generate revenue.

Organizations might perform this risk assessment by using techniques that fall into two different categories: qualitative techniques and quantitative techniques.

**QUALITATIVE RISK ASSESSMENT**

Qualitative risk assessment uses the subjective judgment of experts to evaluate the likeli­hood and impact of risks facing the organization. The process used to create a qualitative risk assessment can range significantly, depending upon the sophistication of the organization. Some organizations with advanced risk assessment capabilities have standing executive com­mittees that meet regularly to discuss and evaluate risks. In less formal approaches, several experts at lower levels in the organization might work together to develop a qualitative risk assessment.

Regardless of the approach, qualitative assessments rely upon the judgment and institu­tional knowledge of these individuals to rank risks based upon the likelihood that they will occur and the impact on the organization if they do. The most common approach is to assign each risk a rating of “high,” “moderate,” or “low” for both likelihood and impact. The results can then be visually portrayed in a matrix similar to the one shown in Figure 1-3.

Une image contenant table

Description générée automatiquement

FIGURE 1-3 A matrix such as this can be used for qualitative risk assessment.

Using this type of visual approach for a qualitative risk assessment allows decision-makers to easily grasp the priority of addressing each risk. In the matrix shown in Figure 1-3, it is apparent that the greatest risk facing the organization is a denial of service attack on the website (high likelihood, high impact). If the organization’s chief information officer is trying to decide between investing in availability controls that will reduce the likelihood that the risk will materialize or purchasing anti-theft devices for encrypted laptops, she will be able to make the decision easily after reviewing the qualitative risk assessment. Improving the availability controls addresses a much more significant risk than protecting encrypted laptops against theft (low likelihood, low impact).

**QUANTITATIVE RISK ASSESSMENT**

Quantitative risk assessments take a more rigorous approach, using numeric data to perform risk calculations in terms of financial value. This requires the use of several factors and formulas:

Organizations must first identify the asset value (AV) for each asset covered by the risk assessment. AV is normally expressed in terms of dollar value. This can be done by using a variety of valuation techniques, such as purchase price, replacement cost, or depreciated value. It’s a good idea to consult your organization’s financial division to ensure that the asset valuation technique used in your risk assessment process is consistent with organizational standards.

*NOTE DETERMINING ASSET VALUE Identifying the value of an asset can be quite difficult, especially for information assets. It’s easy to put a value on a server by using either the purchase price or replacement cost. But what is the value of a list of employee Social Security numbers (SSNs)?  
 One way of valuing such intangible assets is to estimate the costs you would incur if the information were disclosed or lost.*

For each risk facing an asset, the risk assessment process next identifies the exposure factor (EF). The exposure factor is the amount of damage that would occur to an asset if the risk were to materialize; this is normally expressed as a percentage. For example, if the risk of fire is likely to destroy half of a data center, the EF is 50 percent.

The last input into the quantitative risk assessment process is the annualized rate of occurrence (ARO). This is the likelihood that the risk will materialize, expressed as the number of times the risk is expected to occur in a typical year. The value may be less than one if the risk is expected less than once per year. For example, a business located in a 100-year flood plain expects flooding once every 100 years. The ARO for this risk would be 1 in 100, or 0.01.

Next, the risk assessment process calculates the single loss expectancy (SLE). This is the impact of the risk, expressed as the financial loss that occurs each time the risk materi­alizes; it is calculated by using this formula:

SLE = AV × EF

Finally, the risk is calculated as the product of likelihood (ARO) and impact (SLE) by using this formula:

ALE = SLE × ARO

This formula provides the annualized loss expectancy (ALE), or the expected financial loss that will occur due to the risk in a typical year.

*NOTE CLOUD COMPUTING RISKS*

*The rapid adoption of cloud computing services in many organizations poses new risks that must be brought into the risk assessment process. If you use cloud services in your organization, you should ensure that your process includes the identification and assessment of cloud-related risks, including:  
 Information being stolen from the cloud provider.   
 Another user of a shared cloud service gaining access to your data stored on a shared server.   
 The cloud provider suddenly going out of business, leaving you unable to access your data.  
 An outage at the cloud provider causing them to violate their service level agreement (SLA).   
 The activity of another customer in the cloud service causing service degrada-tion that disrupts your service.*

*Let’s work through an example of quantitative risk assessment. Consider a data center lo­cated in the San Francisco Bay Area. Risk managers for the firm owning the data center would certainly be interested in assessing the risk associated with an earthquake damaging the data center. Here’s the process they would go through to do this by using quantitative techniques:*

Identify the asset value (AV). They might do this by consulting data center construction experts and determining that the replacement cost of the data center would be $20 million. (AV = $20 million)

Determine the exposure factor (EF). Consulting with those same experts might iden­tify that the data center would be half destroyed by a significant earthquake. (EF = 50 percent)

Identify the annualized rate of occurrence (ARO). This is the likelihood of an earth­quake occurring in a particular year. The US Geological Survey estimates that the Bay Area is likely to suffer an earthquake causing extensive damage once every 30 years. (ARO = 0.03)

Calculate the single loss expectancy (SLE). This is the impact of an earthquake, expressed as the financial loss that a single earthquake would create, and is calculated as the prod­uct of the asset value and exposure factor:

SLE = AV × EF SLE = $20 million × 50 percent SLE = $10 million

Calculate the annualized loss expectancy (ALE). This is the risk, expressed as the finan­cial loss from earthquakes expected in a typical year:

ALE = SLE × ARO ALE = $10 million × 0.03 ALE = $300,000

A risk manager can now use the annualized loss expectancy to make risk-based decisions. For example, an earthquake insurance policy with a $50,000 annual premium would be a good investment!

**MANAGING RISK**

After an organization completes a risk assessment, it has a clear picture in quantitative and/or qualitative terms that allows it to prioritize the risks facing the organization. Security professionals must then take action to manage those risks. They have five options at their disposal: risk avoidance, risk transference, risk mitigation, risk deterrence, and risk acceptance. They can select one or more of these strategies for each risk identified in the risk assessment.

**RISK AVOIDANCE**

In a risk avoidance strategy, the organization changes its business activities to avoid the risk entirely. For example, an organization considering the earthquake risk described in the quan­titative risk assessment section of this chapter might decide that the risk is simply too high to justify and decide to relocate the data center to an area that is not threatened by earth­quakes. In other cases, an organization might be able to stop performing a particular activity that creates risk. For example, an organization concerned about the theft of Social Security numbers might decide to stop collecting them and purge them from its databases.

Risk avoidance is often a dramatic step that involves significant time and expense to imple­ment. In many cases, business requirements prevent the use of this strategy because of the dis­ruption of necessary business activity. For example, a credit card processing company cannot decide to entirely avoid the risk of handling highly sensitive credit card information without going out of business!

**RISK TRANSFERENCE**

Risk transference moves the impact of a risk from one entity to another. The most common form of transferring risk is the purchase of an insurance policy where, in exchange for a peri­odic premium payment, an insurance company agrees to accept the financial risk associated with an asset or activity. Businesses often purchase insurance policies for fire, accident, theft, and other risks. It is also becoming more common to see organizations purchase insurance that protects against information security liabilities.

Another form of risk transference takes place when two entities sign a contract that contains an indemnification clause. When placed into a contract, an indemnification clause specifies the terms under which one entity will assume responsibility, especially financial responsibility, for a particular type of liability. For example, a company that provides you with cloud services might indemnify you against the risk that their software violates the intellectual property of a third party. In the event that a third party later attempted to sue you for damages, the indemnification clause of your contract would transfer liability for those damages to the cloud provider.

**RISK MITIGATION**

The most common risk management strategy followed by information security professionals is risk mitigation. In this strategy, security professionals use controls designed to reduce the likelihood that a risk will affect an organization and/or the impact that a risk will have on the organization if it materializes.

When an organization decides to adopt a risk mitigation approach, it designs and imple­ments one or more security controls that can be directly mapped to that risk. For example, an organization seeking to reduce the risk of network intrusion might decide to install a network firewall, a network intrusion prevention system, and monitoring software. Each of these three controls can then be directly mapped to the risk of network intrusion.

**RISK DETERRENCE**

In some cases, the organization might be able to adopt a strategy of risk deterrence. This ap­proach uses measures designed to reduce the likelihood that a threat will surface. The most common example of deterrence is used to thwart criminal activity by counter-threatening with an aggressive reaction stance. For example, an organization might aggressively pros­ecute individuals who attempt to intrude into computer systems without permission. Similarly, the owners of a physical facility might have vicious guard dogs on site that threaten intruders with bodily harm. This strategy, used judiciously, can be highly effective, because criminals looking for a target of opportunity will simply go elsewhere.

**RISK ACCEPTANCE**

In some cases, an organization might decide that risk acceptance is the most appropriate strategy for managing a particular risk. In this scenario, after careful evaluation, the organiza­tion decides that the most prudent course of action is to simply monitor the evolution of a risk. Cost or operational concerns dictate that the organization cannot or should not avoid, mitigate, transfer, or deter the risk, so no further action is taken.

**SECURITY CONTROLS**

As mentioned in the previous section, security professionals spend a large amount of their time developing ways to mitigate risks facing an organization’s information assets. The meth­ods they develop to reduce risk are known as security controls and are grouped into three categories: technical controls, operational controls, and management controls. A balanced approach to information security combines controls from each of these categories to mitigate a wide variety of risks.

**TECHNICAL CONTROLS**

Technical controls, as the name implies, leverage technology to reduce the likelihood or impact of a risk on an organization. These controls are typically implemented with the advice and consultation of security professionals and are then maintained either by security profession­als, system administrators, network engineers, database administrators, or other technical staff with the appropriate skillset.

Examples of technical controls abound in the security industry. Firewalls, intrusion detec­tion systems, and wireless encryption are examples of technical controls used in network security. Antivirus software, full disk encryption, and user authentication are examples of technical controls for host security. Transport encryption, input validation, and role-based access are examples of application-oriented technical controls. Most organizations with a well-developed security program can likely list dozens of individual technical controls in place to mitigate various security risks.

**OPERATIONAL CONTROLS**

Operational controls are similar to technical controls in that they directly impact information systems, but the job of carrying out an operational control is primarily done by individu­als, rather than technology. For example, although implementing access control systems is a technical control, performing periodic reviews of user rights and permissions is an operational control. Similarly, the process of business continuity planning, which is discussed in Chapter 4, is an operational control. Other operational controls include conducting routine information security audits, implementing change and configuration management procedures, ensuring physical security, and conducting background checks and other personnel security measures.  
 **MANAGEMENT CONTROLS**

Management controls are those controls focused on the risk management process itself.   
They ensure that the risk management process is running effectively and, therefore, have an indi­rect impact on the security of an organization’s information assets. Operational and technical controls, on the other hand, directly impact those assets.

Examples of management controls include conducting periodic risk assessments and secu­rity control assessments, following a security planning process, and protecting the security of the system and services acquisition life cycle.

**INCIDENT RESPONSE**

Though security professionals strive to ensure that risk management and control processes prevent breaches of confidentiality, integrity, and availability, it is simply impossible to build a completely secure system. A determined (or lucky) attacker can often find a way to bypass even the most sophisticated control systems. Therefore, security professionals must also develop, train on, and implement sound incident response procedures to activate in the event of an information security incident. In this section, you’ll learn the building blocks of a solid incident response program.

Real world Advanced persistent threats If you’re wondering whether it is really possible to breach your well-designed security controls, consider the risk posed by the advanced persistent threat (APT). In this scenario, a determined attacker with tremendous resources focuses on breaching the security controls of your organization in particular. Although you certainly may have designed your defenses in such a way that they will easily foil the determined attacker, would you be able to defend against someone who carefully studies your organization, perhaps with insider knowledge, and then dedicates a team of highly skilled individuals with advanced tools to penetrating your defenses? Though this might sound far-fetched, it’s exactly what happened to a nuclear enrichment plant in Iran that was the victim of the Stuxnet attack. In the Stuxnet case, a group of dedicated programmers spent several months developing a worm with one pur-pose—to work its way into the central control systems of the plant to destroy the centrifuges. Although no government has publicly taken credit for the attack, it is widely assumed that the United States and/or Israel was behind it.

**INCIDENT RESPONSE TEAM**

Appropriately responding to an information security incident requires the carefully coordi­nated actions of a team of highly skilled individuals who have been trained on the organiza­tion’s consistent process for incident response. This is simply not something that you can pull together “on the fly.” Success during a security incident requires careful advance planning, including the selection and training of an incident response team.

**FIRST RESPONDER RESPONSIBILITIES**

It’s important to recognize that the first responders on the scene of an information security incident will most likely not be members of your trained incident response team. The first person to notice the sign of an information security incident is more likely going to be a system administrator, computer operator, or even an end user. For this reason, you should consider every member of your staff to be a member of your “extended” incident response team and provide some level of training across the organization. There are three basic ele­ments to this training:

Recognizing a security incident Everyone in the organization should have an understanding of what constitutes a security incident in the eyes of your firm.

Activating the incident response process Next, first responders should have a clear, easy way to activate your formal incident response process. It should be simple for them to, in a sense, dial your “information security 911” to have trained profession­als jump into action to assume control of the incident.

Containing the incident Finally, most technical staff in your organization should know how to perform the equivalent of “information security first aid.” Just as a by­stander wouldn’t stand by and wait for an ambulance while an accident victim bled profusely, IT staff should feel confident enough to take immediate action to stem the effect of a security incident. Actions as simple as disconnecting the network cable from a system that appears to be transmitting unencrypted credit card data to an offsite lo­cation can mean the difference between a minor and major security incident. Seconds matter when it comes to the early stages of incident response.

NOTE DON’T SHOOT THE MESSENGER When you train large portions of your staff on first responder tactics, understand that they will make mistakes. Staff members will jump the gun and activate the incident response process in cases where there simply is no security incident. The way your organization reacts to these mistakes is just as important as your response to a true security incident. If the person who activated the process feels belittled or punished in any way, he will hesitate to ever again activate the incident response process. Even worse, others in the organization will hear the story, and it will give them pause as well. No matter what, you should always thank first responders for bringing a potential incident to your attention and make sure they understand that they made the right decision calling in the incident response team.

Of course, the level of detail that you provide should vary depending upon the role of the individuals within your organization. Staff members with no technical responsibilities what­soever might simply get an awareness message letting them know that they should report any suspicious computer activity to a centralized security operations center or network team. System and network administrators might receive a full day of training that helps them un­derstand how to recognize the early warning signs of a security incident and the basic steps that should be followed during incident containment.

**STAFFING THE INCIDENT RESPONSE TEAM**

Responding to an information security incident requires an interdisciplinary approach that will call upon the expertise of many different professionals from throughout your organization. Remember, responding to security incidents is not just an “infosec thing,” nor is it purely a technical matter. Although information security professionals and other technical staff play an important role in incident response, it is equally important to have a well-rounded team that can handle all aspects of incident response.

There are eight categories of staff that you should consider representing on your incident response team. This does not necessarily mean that you will only have eight slots on the team, for two reasons. First, you need to plan to have a redundant team. If the attorney on your team is vacationing in Barbados when an incident occurs, you need to know that there is someone else available who can represent the legal issues. Second, some areas are broad enough that no one person can represent the entire field. For example, a network engineer would not likely be able to address database administration issues, nor would a database ad­ministrator be able to cover network issues. The categories of staff you should consider when developing your team are:

Management Quite simply, somebody needs to be in charge. Incident response without one officially designated leader can quickly devolve into many uncoordi­nated efforts, as everyone begins to pursue their own hunches and preferred courses of action. You need one strong leader to rein in these natural tendencies and direct the response. Additionally, difficult decisions will be made during the response to an information security incident, and you need to be sure that the team has a manager on hand with sufficient authority to make those calls without having to call in senior managers for consultation.

Information security Information security staff will play an essential role in all stages of incident response. They bring subject matter expertise to the table that can be especially helpful when attempting to identify the root cause of an incident or to quickly develop ad hoc controls to contain the damage caused by a security incident. Security staff also have access to unique resources, such as firewalls, intrusion detec­tion/prevention systems, and security incident and event management (SIEM) systems that might contain data relevant to the security incident.

Technical staff In addition to information security professionals, you should have a representative from every major technical discipline in your organization on the incident response team. You certainly might not need all of these staff to respond to every incident, but you need to be prepared to react to a security incident that touches any part of your computing environment. System administrators, network engineers, database administrators, and application developers all might play critical roles in responding to an incident that either centers on or touches upon their opera­tional domains.

Legal Many security incidents turn into legal matters, either because criminal pros­ecution is involved or because the firm becomes engaged in civil litigation as a con­sequence of the security incident. In addition, there are specific legal provisions that might dictate elements of your incident response process. For example, most states now have data breach notification laws that require the timely notification of individu­als if their data is known or reasonably believed to have been compromised during an information security incident.

Communications and public relations You might need to issue some type of pub­lic statement, and you will need to react if the media gets wind of the fact that a secu­rity incident is unfolding at your organization. Communications staff should become involved early both to handle these situations and provide advice on the best time to inform outsiders that an incident is taking place.

Human resources In any incident where insider involvement is suspected, you should include representatives from your human resources department. You should definitely consult HR before interviewing any suspects who are employees of the or­ganization. HR should also lead any disciplinary process that might take place against employees who are believed to have been involved in the incident, because such inves­tigations are personnel matters that are within their realm of expertise.

Risk management Your organization’s risk management staff will play an impor­tant role in security incidents of extended duration or impact. Individuals from this group will likely be the experts on your firm’s business continuity and disaster recovery strategies and can help implement those contingency plans if it becomes necessary. Additionally, staff from the risk management area will be able to best inform the team on the provisions of any insurance policies that might cover portions of the incident response measures.

Facilities If physical security is involved in a security incident, your facilities group can provide important expertise regarding your buildings and other physical infra­structure.

Developing a well-rounded incident response team is an important component of any strong incident response program. You should identify individuals to fill each of these roles and ensure that they understand the scope of their incident response functions.

NOTE OUTSOURCING INCIDENT RESPONSE Many organizations are turning to outsourced providers to perform a variety of informa-tion technology functions, and incident response is no exception. Although it is possible to outsource your entire incident response program to an outside provider, this is uncom-mon, because some degree of institutional knowledge is critical to a successful response. However, it is certainly possible to outsource components of incident response, especially where very specialized technical skills are required. For example, you might not have use of a full-time computer forensics investigator on your staff if those skills are only required a few times a year. Instead, you might retain a forensics firm with a rapid response capabil-ity and have them perform this role on an as-needed basis. If you do choose to outsource components of incident response, remember that making these arrangements in advance should be a part of your incident response planning process. You don’t want to wait until an incident is underway to try to identify and contract with a forensics firm. You should al-ready have a contract signed so that you can simply activate the resource when you need it.

**TRAINING THE INCIDENT RESPONSE TEAM**

The training you provide to your incident response team should cover a wide variety of topics that prepare the team members to handle different types of information security incidents. This training should include a core set of modules that all team members receive, covering the following topics:

* Overview of the organization’s incident response process
* Roles and responsibilities of each team member
* Activation procedures in the event of an incident
* Detection and analysis of security incidents
* Containment procedures
* Eradication procedures
* Recovery procedures
* Post-incident procedures

In addition, each team member should receive specialized training on the incident response tools and techniques specific to her area of expertise. For example, database and system ad­ministrators should be familiar with their roles in a forensic analysis, including proper collection procedures and the chain of custody. Attorneys should have specialized continuing legal education on the laws and regulations that pertain to information security incidents.

All of these training modules should be conducted on both an initial and recurring basis. If you are developing a new incident response capability, you could have large group sessions to bring the entire team up to speed at once. If you are maintaining an existing program, you will need to conduct initial training sessions for those staff members who are new to the incident response team. Additionally, you will need to conduct periodic refresher training for veteran team members to ensure both that they don’t get “rusty” and that they become familiar with any changes in the incident response plan.

Finally, a critical component of any training program is giving responders hands-on experi­ence. This is especially important in organizations that do not often activate their incident response teams. Conducting a series of drills can help familiarize staff with their roles in an actual incident. These drills can range from checklist reviews to tabletop exercises or even full-blown incident simulations.

**INCIDENT RESPONSE LIFE CYCLE**

Every incident response process follows a life cycle approach, whether it is formally de­fined or not. The National Institute of Standards and Technology (NIST) defines one such life cycle approach, using the four-phase process shown in Figure 1-4. This includes four distinct phases:

* Preparation
* Detection and analysis
* Containment, eradication, and recovery
* Post-incident activity

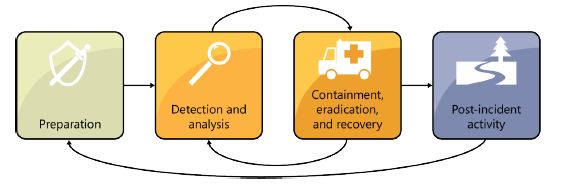


FIGURE 1-4 The incident response life cycle contains four steps (NIST).

Each of these stages has goals and objectives that will be discussed in the next several sections of this chapter. Also, be sure to take note of the multiple arrows and their directions in Figure 1-4. The incident response life cycle is not a sequential march through four phases. Rather, it is an iterative process that might loop through some steps multiple times as an inci­dent evolves. Most notably, the steps taken during the containment, eradication, and recov­ery phase might identify additional information that requires analysis, causing a loop back to the detection and analysis phase.

Additionally, the entire process should be viewed as a repeating cycle. At the conclusion of each incident, you engage in post-incident activity that includes a lessons-learned session assessing the functioning of the incident response process. This information then feeds back into the preparation phase, providing valuable input regarding potential improvements to your organization’s incident response process.

**PREPARATION**

The preparation phase of incident response includes establishing an incident response process, selecting a team, and training them on the plan. These steps were described earlier in this chapter.

In addition to those preparation steps, the incident response team members should ensure that they have the tools and resources needed to respond to any eventuality. Many teams choose to create a “go bag” that contains all of the tools needed to get an incident response underway quickly. At a minimum, the “go bag” should contain a forensic laptop, a variety of cables and connectors, several types of blank media for imaging systems, and other essential gear required by members of the response team. The “go bag” should be considered sacro­sanct and should be inventoried periodically to ensure that nobody has “borrowed” equip­ment from the kit. You don’t want to activate the team and get on site only to discover that essential equipment was purloined temporarily for a project and is not actually in the kit.

In addition to the incident response life cycle, NIST offers a suggested list of tools and re­sources that should be maintained by incident response teams. They suggest that every team have access to the following:

Communications and facilities resourcesContact information for team members, other internal resources, law enforcement contacts, and contractors

On-call information for other teams within the organization that might play a role in incident response

Incident reporting mechanisms

Issue tracking system

Smartphones

Encryption software for intra-team communication and collaboration with outside parties

A permanent or temporary war room to act as a central coordination point during incident response

A secure storage facility for evidence gathered during an incident response effort

■Incident analysis hardware and software Digital forensic workstations and/or backup devices to create disk images and pre­serve other types of digital evidence

Laptops for team member use that are separate from the forensic workstations

Spare equipment for use during the response, including workstations, servers, and network gear

Blank removable media (lots of it!)

Removable media loaded with forensic tools (potentially including bootable images)

A printer

Packet-sniffing and network protocol analysis hardware and software

Forensic software

Notebooks, cameras, recorders, and other equipment to gather evidence and notes

■Incident analysis resourcesNetwork diagrams

Lists of critical information assets

Architectural diagrams, especially of critical/sensitive services

Baselines of “normal” system, network, and application activity

A detailed listing of firewall rules and ports

Many teams have a full-time incident response coordinator (often a member of the infor­mation security team) who is responsible for gathering resources and ensuring that every­thing is ready to go in the event of an actual incident. This coordinator might also facilitate the incident response planning, training, and simulation processes for the organization. Smaller organizations might choose to make this a part-time responsibility for a team member with other information security duties.

**DETECTION AND ANALYSIS**

The detection and analysis phase has two distinct components. First, during periods of nor­mal activity, trained security analysts monitor systems for signs of a security incident. This may include monitoring:

* Intrusion detection and prevention systems.
* Security incident and event management (SIEM) systems.
* Firewalls.
* Centralized antivirus monitoring software.
* Logs from critical systems, applications, and devices.
* File/system integrity monitoring software.
* Vulnerability scanners.
* External reports of malicious activity (for example, attacks emanating from your network).
* Reports from staff and customers.

Analysts monitoring these sources for signs of an information security incident will activate the formal incident response process in the event that they detect an incident.

When an incident is detected, analysts are responsible for gathering enough information to guide the response effort. This can involve coordinating information from the same sources used to detect the incident as well as activating additional information collection mechanisms. For example, analysts might begin capturing network traffic in real-time by using packet sniffers to preserve evidence of a network-related incident.

Another important part of the analysis phase is assessing the impact of the incident. This can be done by classifying the event into one of three categories:

Low impact Incidents that have minimal or no potential to affect the confidentiality, integrity, or availability of the organization’s operations and/or information assets. It is unlikely that a low-impact event would warrant a major after-hours response or the activation of the full incident response team.

Moderate impact Incidents that have the potential to have a significant impact on the confidentiality, integrity, or availability of the organization’s operations and/or information assets. They might disrupt some business activities and might require the activation of the incident response team.

High impact Incidents that have the potential to critically damage the confidential­ity, integrity, or availability of the organization’s operations and/or information assets. They might have a very serious, potentially permanent, impact on the organization and should entail immediate activation of the full incident response team.

Every organization will need to define its own criteria for triaging security incidents and determining the incident categorization scheme appropriate for its environment. Those cri­teria will vary depending upon the types of information handled by the organization and the criticality of various business processes supported by information technology.

**CONTAINMENT, ERADICATION, AND RECOVERY**

The containment, eradication, and recovery phase of an incident response typically encom­passes what most security professionals consider to be the “meat” of the process. It includes steps taken to minimize the damage caused by a security incident, remove the threat, and return to normal operations. Though incident response guides typically describe this as a single phase, it is clearly divided into two different types of complementary activities: containment activi­ties and eradication/recovery activities.

**CONTAINMENT ACTIVITIES**

Containment activities are focused on damage control and preventing further loss to the organization. The steps followed will vary depending upon the type of incident taking place and the technical countermeasures available. Some examples of security incident containment strategies include:

* Provisioning additional bandwidth to cope with the impact of a network denial of service attack.
* Disconnecting a potentially compromised server from the network to prevent the exfil­tration of sensitive information.
* Isolation of a network segment to prevent further spread of malware that has infected systems on that segment.
* Creating temporary firewall rules to block external access to a system that is acting suspiciously.

Security professionals must work closely with other technical staff during containment activities to design a containment strategy that appropriately balances the needs of the organization with security concerns. Your organization should maintain an incident contain­ment plan for each of the major types of attack in your planning scheme to allow for advance planning in as many situations as possible.

NIST offers six criteria that incident response planners and teams can use when developing an appropriate containment strategy:

* Potential damage to and theft of resources
* Need for evidence preservation
* Service availability (for example, network connectivity or services provided to external parties)
* Time and resources needed to implement the strategy
* Effectiveness of the strategy (for example, partial containment or full containment)
* Duration of the solution (for example, an emergency workaround to be removed in four hours, a temporary workaround to be removed in two weeks, or a permanent solution to the problem).

Another important consideration is that containment strategies are likely to alert an at­tacker to the fact that security responders have detected his activity. This might cause an immediate termination of the attack. Although this is certainly good from the perspective of preventing further damage, it limits the ability of responders to gather evidence that can be used to track down and prosecute offenders. The incident response plan should contain guidelines to help teams make these determinations. Incident response team leaders should en­sure that all staff participating in a response understand the incident’s situation-specific rules of engagement regarding the relative priorities assigned to containment and evidence collection.

**ERADICATION AND RECOVERY ACTIVITIES**

Eradication and recovery activities also take place during this phase and are focused on removing any aftereffects of the incident and returning the organization to normal technol­ogy operations as quickly as possible. The extent of the activities performed during this phase vary depending upon the type of incident. In some cases, there might be very little work to do. However, in cases where systems were compromised, eradication efforts might involve completely wiping affected systems to ensure that there are no lingering effects from the compromise.

Recovery includes not only restoring normal activity but also ensuring that any vulnerability that might have been exploited by attackers is remediated. If attackers found your vulner­ability once, it is extremely likely that they will be able to do so a second time. You should not consider your operations fully recovered until they are functioning again and the vulner­abilities exploited by attackers are resolved so that they do not continue to pose a risk of compromise.

**POST-INCIDENT ACTIVITY**

The final phase of the incident response process, post-incident activity, consists primarily of a lessons-learned analysis that does a postmortem look at the incident response process. It provides an opportunity for everyone who participated to reflect upon the response and any changes that might benefit future responses. In Special Publication 800-61, NIST suggests a series of questions that can be addressed during a lessons-learned session:

* Exactly what happened and at what times?
* How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
* What information was needed sooner?
* Were any steps or actions taken that might have inhibited the recovery?
* What would the staff and management do differently the next time a similar incident occurs?
* How could information sharing with other organizations have been improved?
* What corrective actions can prevent similar incidents in the future?
* What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

The session conducted to answer these questions should have a designated facilitator who moderates the conversation. This person should have enough incident response experience to ask the appropriate follow-up questions and guide the exploration, but should not have been involved in the actual response, to preserve a sense of objectivity. It can also be helpful to have a dedicated note-taker to ensure that everyone’s input is accurately captured. At the con­clusion of the meeting, the facilitator should prepare a lessons-learned report that highlights the major findings of the session and key lessons learned that might benefit responders to future incidents. This document should be used to make revisions to the incident response process.

**INCIDENT COMMUNICATIONS**

During an incident response, the team might need to communicate with a wide range of external parties, as shown in Figure 1-5. These are individuals who either need to be informed of the incident or might provide information valuable to the response effort. All external com­munications should be coordinated through the communications lead on the incident response team to ensure that the team is presenting consistent information to the outside world.

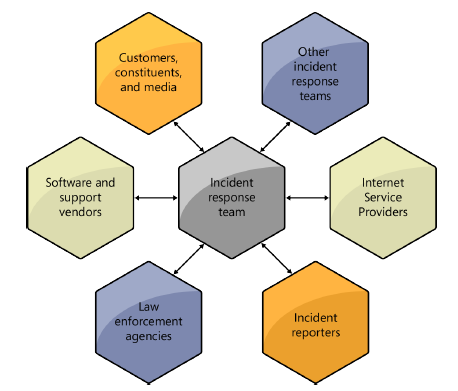


FIGURE 1-5 The incident response communications process suggested by NIST uses the incident response team as the core of all communications (NIST).

Some of the particular entities that the incident response team might communicate with include:

Customers, constituents, and the media There are many stakeholders who will be interested in learning about the potential loss of sensitive information or who are oth­erwise affected by the incident. These communications must be coordinated through your public relations group.

Other incident response teams If you are responding to an incident that affects multiple organizations, such as a widespread distributed denial of service (DDoS) at­tack, all responders will benefit from opening channels of communication between each organization’s response team. This information sharing might help uncover im­portant information more quickly and allows for a coordinated response.

Internet Service Providers (ISPs) In a network-based incident, your ISP might be able to provide important information or implement strategies to help you contain the incident. For example, the ISP might be able to implement filtering that prevents traffic related to a DDoS attack from reaching your network in the first place.

Incident reporters You might decide to report the incident to a state, national, or industry-specific incident response team. US federal government agencies are required to report security incidents to the United States Computer Emergency Readiness Team (US-CERT).

Law enforcement agencies Depending upon the nature of the incident, you might be required to involve law enforcement or you might choose to voluntarily do so. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires that merchants suspecting a security incident that involves credit card information must immediately alert both their merchant bank’s fraud unit and the United States Secret Service.

Software and support vendors You might need support from your vendors to diagnose and/or remediate the effects of a security incident.

Your incident response plan should include the procedures to be followed when involv­ing each of the types of organizations listed here. It should describe who has the authority to initiate each contact during a security incident and should also contain contact informa­tion for each entity.

**COLLECTING EVIDENCE**

Every incident response effort involves some form of evidence collection. In some cases, the evidence gathered is used solely by the incident response team. In other incidents, evi­dence might be turned over to the organization’s legal team for use in civil litigation, or to law enforcement for use in a criminal prosecution. In cases where evidence is used outside of the incident response team, it is absolutely critical that it be collected by following established evidence handling procedures. Evidence that is mishandled might be inadmissible in court.

**PRESERVING THE CHAIN OF CUSTODY**

One of the most important aspects of evidence collection is preserving the evidence chain of custody. This means that you must create a paper trail that documents the history of the evi­dence from the time of collection until the moment it is used in court. This is done by using an evidence log that contains the following data elements:

Identifying information that describes the nature of the evidence. This might include model numbers, serial numbers, IP/MAC addresses, user names, or other similar infor­mation.

A description of the collection process used to gather the evidence, including contact information for the technician who collected it.

Entries for every time the evidence was handled after collection. Each entry must include the name and contact information of the individual handling the information, the purpose for handling the evidence, and the location where it was stored after it was handled.

Quite simply, the chain of custody should tell a complete story of the life of the evidence. The evidence log should explain every single thing that happened to the evidence during and after collection, and it should document both the physical location of the evidence at all times and the names of any individuals who came into direct contact with it. The purpose of the chain of custody is to ensure that officials can provide definitive documentation of their evidence and ensure that it was not tampered with between the time of collection and the time of use.

**INTERVIEWING WITNESSES**

In many incidents, it might become necessary to interview witnesses to gather evidence. Interviews are conducted on a voluntary basis and should have a cooperative tone to them. In­dividuals conducting interviews should not be hostile toward witnesses or attempt to browbeat them into providing information. If either the interviewer or interviewee is uncomfortable with the proceedings, the interview should immediately be terminated. Don’t let interviewers take lessons from police dramas!

Any interview that takes place should be thoroughly documented in a manner that is known to all participants. If the interview subject consents, you might use audio or video recording to document the interview. Otherwise, the interviewer might take paper notes to record the conversation.

Remember, an interview that turns hostile is no longer an interview, but an interrogation. At no time should anyone other than trained law enforcement personnel engage in the inter­rogation of a witness. In the best case, interrogation by untrained individuals might result in evidence that is not usable in court. In the worst case, the interrogator may find himself guilty of a crime.

**TRACKING TIME AND EXPENSE**

Incident response teams should track the time and expenses associated with both evidence collection and other incident response efforts. Though these expenses might not be directly billable to any organization, they provide management with a method of identifying the resources that went into an incident response effort. At the very least, this information can be used to plan for future incident responses. In some cases, management might be able to seek reimbursement through litigation or from an information security incident insurance policy purchased by the organization.

**COMPUTER FORENSICS**

In many cases, investigators responding to an information security incident will need to collect information from computer systems believed to have played a role in the incident. This process, known as computer forensics, includes tools and techniques that ensure that evidence is collected in a manner that does not alter the evidence itself and preserves the chain of custody.

**ORDER OF VOLATILITY**

Unlike many kinds of physical evidence, computer-based evidence is often volatile. This means that it breaks down over time and, if not promptly and properly collected, it will disappear and be impossible to recover. Forensic investigators should consider the order of volatility when collecting evidence. Here’s a summary of major computer evidence types, ordered from highest volatility (shortest life) to lowest volatility (longest life):

* RAM
* Network details
* Running process information
* System disk contents
* Removable flash media
* Removable magnetic media
* Removable optical media

Evidence from the first three elements on this list (memory contents, network details, and running process information) is only available as long as the system containing the evidence has power. For this reason, most organizations have policies specifying that first responders should never unplug a computer believed to be involved in a security incident. Doing so could destroy critical evidence before it is forensically collected. Responders seeking to con­tain the damage caused by a security incident should instead disconnect the system from the network, leaving it powered on. Though this may destroy some network-based evidence, it leaves important memory and process information intact while containing damage.

As forensic analysts develop an evidence collection plan for a security incident, they should begin with the most volatile evidence from categories at the top of this list and work their way downward, collecting the least volatile evidence last. This approach maximizes the amount of data that can be collected before it expires.

**HASHING**

Investigators make use of cryptographic hash values to demonstrate that one file is a true copy of another file. Hashes are values generated by a mathematical function that provide a summary of the contents of one or more blocks of data. Hash functions must be designed in such a way that they are efficient to compute. Additionally, the hash value must be collision resistant, meaning that it should not be mathematically feasible to find two different files that generate the same hash value.

If a hash value is created by using a proper hash function, it can be used to quickly and reliably compare the contents of two files. If the files are identical, they will generate identical hash values. If the hash values generated by two files do not match, then the files themselves differ in some way. It is important to note that hashing does not give you a sense of “how close” the files might be. If a single character in the files is different, the hash values might be completely different. You simply can’t tell by comparing hash values whether a modification to a file was just a single letter or whether the files are completely different.

There are many software products capable of generating hash values for use in forensic examinations. Figure 1-6 shows one of these programs creating a hash value for a system file by using the well-known Message Digest 5 (MD5) hash algorithm.

Une image contenant texte

Description générée automatiquement

FIGURE 1-6 This screen shot demonstrates the creation of an MD5 hash.

**IMAGING SYSTEMS**

One of the most important forms of evidence captured during forensic investigations is system images. These images, gathered by using specialized forensic imaging equipment, are bit-by-bit copies of hard drives from systems involved in a security incident. System im­ages are collected in a manner that ensures that the act of creating the image does not alter the data stored on the hard drive. Forensic investigators typically ensure that this is the case by using specialized forensic devices known as write-blockers. These are hardware connec­tors that sit between the drive being imaged and the hardware performing the imaging and ensure that no data can be written onto the drive, while permitting data to be read from the drive during the imaging process.

One of the major benefits of capturing a bit-by-bit image, rather than copying individual files from the disk, is that you receive a copy of the unused space on the disk. This space might contain portions of deleted files or other information that can prove very significant during the investigation.

Investigators performing forensic analysis never work with original media. After creating the image, investigators seal the original media in an evidence bag and securely store it in an evidence locker, being careful to preserve the chain of custody. This is because the original drive is direct evidence that might be used in court. Furthermore, investigators usually don’t even work with the original image. They maintain it as a master image and make copies of that image for investigative purposes.

NOTE IMAGES AND HASHING With all these images and copies of images, how can a forensic team keep things straight and ensure that they are always working with a real copy of the original media? Through the use of cryptographic hashes! In the previous section, you learned how hashes can be used to verify the contents of a single file. Investigators also use hashes to verify the integrity of disk images. They record a hash of the original disk at the time it is collected and then they can perform a hash of an image at any time. If the hash value of the image matches that collected from the original disk, everyone can be certain that the image is a true copy of the disk that was collected as evidence. This hash verification technique is used in court to demonstrate the reliability of the imaging process and allow investiga-tors to discuss information they gleaned from an image as if they had gleaned it from the original disk.

**NETWORK TRAFFIC AND LOGS**

Network traffic is another important source of information for forensic investigators. In some cases, you might be able to capture the full contents of the data traveling on a network. This technique, known as packet sniffing, monitors a network segment, recording every bit that passes by on the wire, and then reassembles it to provide machine-readable and human-readable forms of the data transmitted on the network.

Analysts can use tools such as the free Wireshark tool shown in Figure 1-7 to capture the full contents of network traffic. It is important to note that capturing live network traffic can quickly consume massive amounts of storage. For this reason, it is extremely unusual to cap­ture network traffic in real time unless there is a known incident taking place. It would simply be cost prohibitive to retain network traffic for any extended period of time.

Une image contenant table

Description générée automatiquement

FIGURE 1-7 This screen shot demonstrates the use of Wireshark to capture network traffic.

Although analysts can’t count on capturing network traffic 24 hours a day, seven days a week for use in a future investigation, there are sources of network data that might be re­tained for extended periods of time. First, many network devices create logs of activity that might contain information useful to a security investigation. For example, the logs on a router might show unsuccessful attempts to create administrative connections to the router that are indicative of an attack in progress. Firewalls might retain logs of permitted and blocked traffic that are useful to security investigators.

The second source of network information that is quite useful to forensic investigators is network flow data. These records, generated by network devices, track summary information about every connection that takes place on a network. They do not capture the full contents of the packet, to avoid the storage space dilemma discussed previously, but they do capture useful summary information, including:

* The source system IP address.
* The destination system IP address.
* The timestamp of the beginning of the connection.
* The timestamp of the end of the connection.
* The amount of data sent from the source system to the destination system.
* The source port for the communication.
* The destination port for the communication.
* The transport layer protocol used for the communication.

This information is enough to provide important details to those investigating a security incident. For example, if a system is known to have been compromised, flow data can be used to identify all of the remote systems that either connected to or were contacted by the com­promised system. Flow data can also be used to disprove theories during a security investi­gation. For example, if a system contains a sensitive file that is 100 megabytes (MB) in size and flow data shows that no connections transmitted more than 25 MB, investigators can be confident that the entire file was not stolen.

**TIME OFFSETS**

It is important to ensure that the system clocks on all computers and devices in an organiza­tion are synchronized.   
This facilitates the analysis phase of security investigations. If clocks are not synchronized, it becomes quite difficult to compare log entries generated by multiple systems.   
Many organizations handle this issue by using the Network Time Protocol (NTP) to ensure that all system clocks are synchronized to one of the atomic clocks maintained by the United States government, or another authoritative source. Access to these clocks is freely available, and the NTP protocol is able to adjust for the network latency between your site and the clock.

If an investigation must take place using information from systems without synchronized clocks, investigators must make use of time offsets. The investigators determine the differ­ence between the clock on each system and the actual time, and then use this as an offset value to adjust the times retrieved from log entries and other timestamps generated by that system. For example, if a system clock is found to be running two minutes fast, analysts must then subtract two minutes from each time value generated by that system to adjust it back to the correct time. This technique can also be used to compare data generated by systems located in different time zones.

**SCREEN SHOTS**

If an investigator encounters a computer that is currently involved in a security incident, that investigator can also use screen shots as a valuable source of evidence. Though it is pos­sible to gather screen shots by using the built-in operating system functionality of the target computer, this is not an advisable technique for a forensic investigator, because the keyboard interaction might be viewed as tampering with the computer itself. One simple solution to this is to simply take a photo of the screen by using a digital camera dedicated to forensic investigations. Remember to timestamp your pictures and subject the clock on the camera to the same time offset procedure used for other systems. Finally, the memory card from the camera must then be treated in the same manner as any other form of digital evidence, with secure storage and a documented chain of custody.

**VIDEO CAPTURE**

Security investigators should also remember to turn to old-fashioned physical security tools when possible. For example, though it might not be possible to digitally determine who is logged onto a computer by using a stolen account, the room containing the computer might contain a surveillance camera that captures a picture of the perpetrator.   
If the room itself does not contain a camera, look for cameras in the hallway, at entrance points, or in other nearby areas that might have captured images of involved individuals.

**CHAPTER SUMMARY**

The goals of information security professionals are to protect the confidentiality, integ­rity, and availability of an organization’s information assets. Adversaries have the cor­responding goals of disclosure, alteration, and denial.

Vulnerabilities are weaknesses in an organization’s security controls. Threats are exter­nal forces that seek to exploit vulnerabilities. Risks occur when there is an intersection between a vulnerability and a threat that can exploit that vulnerability.

Qualitative risk assessment uses a subjective process to evaluate the likelihood and impact of a risk upon an organization. Qualitative assessments commonly use the categories of “low,” “moderate,” and “high” to express these attributes.

Quantitative risk assessment calculates the financial risk that would occur if a risk materialized. It uses the concept of annualized rate of occurrence (ARO) to express likelihood and single loss expectancy (SLE) to express impact. Risks are calculated by using the annualized loss expectancy (ALE).

Organizations have five strategy options at their disposal when determining how to manage a risk: risk acceptance, risk avoidance, risk mitigation, risk transference, and risk deterrence. They can use one or more of these strategies in response to each risk they face.

Security professionals use controls to mitigate risk. These controls can reduce the likeli­hood and/or impact of a risk and are grouped into three categories: management controls, operational controls, and technical controls.

Every organization should have a trained incident response team prepared to react in the event of an information security incident. This team should include technical, legal, communications, and management representatives that will join forces to coordinate a response.

The incident response life cycle has four phases: preparation to get the team ready for future incidents, detection and analysis of an incident; containment, eradication, and recovery; and post-incident activity.