Chapter 16

Disaster Recovery Planning

THE CISSP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

- **Business Continuity and Disaster Recovery Planning**
    - Understand business continuity requirements
        - Develop and document project scope and plan
    - Conduct business impact analysis
        - Identify and prioritize critical business functions; determine maximum tolerable downtime and other criteria; assess exposure to outages (e.g., local, regional, global); define recovery objectives
    - Develop recovery strategy
        - Implement a backup storage strategy (e.g., offsite storage, electronic vaulting, tape rotation); recovery site strategies
    - Understand disaster recovery process
        - Response; personnel; communications; assessment; restoration
    - Provide training
    - Test, update, assess and maintain the plan (e.g., version control, distribution)
- **Operations Security**
    - Manage incident response
        - Detection; response; reporting; recovery; remediation

In the previous chapter, you learned the essential elements of business continuity planning (BCP)—the art of helping your organization avoid business interruption as the result of an emergency or disaster. Recall that a primary BCP principle is risk management; you must assess the likelihood that a vulnerability will be exploited and use that likelihood to determine an appropriate allocation of resources to combat the threat.

Because of this risk management principle, business continuity plans do not seek to prevent every possible disaster from affecting an organization—that is impossible. On the contrary, they are designed to limit the effects of predictable, more likely disasters. Naturally, this leaves an organization vulnerable to interruption from any number of threats—those judged unworthy of mitigation or those not anticipated.

Disaster recovery planning (DRP) steps in where BCP leaves off. When a disaster strikes and a business continuity plan fails to prevent interruption of business activities, the disaster recovery plan kicks in and guides the actions of emergency-response personnel until the end goal is reached, which is to see the business restored to full operating capacity in its primary operations facilities.

While reading this chapter, you may notice many areas of overlap between the BCP and DRP processes. Indeed, our discussion of specific disasters provides information on how to handle them from both BCP and DRP points of view. This illustrates the close linkage between these two sets of activities and processes. In fact, although the (ISC)^2 CISSP curriculum draws a distinction between these two areas, most organizations simply have a single team and plan to address both business continuity and disaster recovery concerns in an effort to consolidate responsibilities. In many organizations, in fact, the single discipline known as business continuity management (BCM) encompasses BCP, DRP, and incident management under a single umbrella.

The Nature of Disaster

Disaster recovery planning brings order to the chaos that surrounds the interruption of an organization’s normal activities. By its very nature, a *disaster recovery plan* is implemented only when tension is high and cooler heads might not naturally prevail. Picture the circumstances in which you might find it necessary to implement DRP measures—a hurricane destroys your main operations facility, a fire devastates your main processing center, terrorist activity closes off access to a major metropolitan area. Any event that stops, prevents, or interrupts an organization’s ability to perform its work tasks is considered a disaster. The moment that IT becomes unable to support mission-critical processes is the moment DRP kicks in to manage the restoration and recovery procedures.

A disaster recovery plan should be set up so that it can almost run on autopilot. The DRP should also be designed to eliminate decision-making activities during a disaster as much as possible. Essential personnel should be well trained in their duties and responsibilities in the wake of a disaster and also know the steps they need to take to get the organization up and running as soon as possible. We'll begin by analyzing some of the possible disasters that might strike your organization and the particular threats that they pose. Many of these are mentioned in the previous chapter, but we now explore them in further detail.

To plan for natural and unnatural disasters in the workplace, you must first understand their various forms, as explained in the following sections.

Natural Disasters

Natural disasters reflect the occasional fury of our habitat—violent occurrences that result from changes in the earth's surface or atmosphere that are beyond human control. In some cases, such as hurricanes, scientists have developed sophisticated predictive models that provide ample warning before a disaster strikes. Others, such as earthquakes, can cause devastation at a moment's notice. A disaster recovery plan should provide mechanisms for responding to both types of disasters, either with a gradual buildup of response forces or as an immediate reaction to a rapidly emerging crisis.

Earthquakes

Earthquakes are caused by the shifting of seismic plates and can occur almost anywhere in the world without warning. However, they are far more likely to occur along known fault lines that exist in many areas of the world. A well-known example is the San Andreas fault, which poses a significant risk to portions of the western United States. If you live in a region along a fault line where earthquakes are likely, your DRP should address the procedures your business will implement should a seismic event interrupt your normal activities.

You might be surprised by some of the regions of the world where earthquakes are considered possible. TABLE 16.1 shows parts of the United States (and U.S. territories) that the Federal Emergency Management Agency (FEMA) considers moderate, high, or very high seismic hazards. Note that the states listed in the table include 82 percent (41) of the 50 states, meaning that the majority of the country has at least a moderate risk of seismic activity.

Table 16.1 Seismic hazard level by U.S. state or territory

Moderate Seismic Hazard	**High Seismic Hazard**	**Very High Seismic Hazard**
Alabama	American Samoa	Alaska
Colorado	Arizona	California
Connecticut	Arkansas	Guam
Delaware	Illinois	Hawaii
Georgia	Indiana	Idaho
Maine	Kentucky	Montana
Maryland	Missouri	Nevada
Massachusetts	New Mexico	Oregon
Mississippi	South Carolina	Puerto Rico
New Hampshire	Tennessee	Virgin Islands

New Jersey
New York
North Carolina
Ohio
Oklahoma
Pennsylvania
Rhode Island
Texas
Vermont
Virginia
West Virginia
Utah
Washington
Wyoming

Floods

Flooding can occur almost anywhere in the world at any time of the year. Some flooding results from the gradual accumulation of rainwater in rivers, lakes, and other bodies of water that then overflow their banks and flood the community. Other floods, known as *flash floods*, strike when a sudden severe storm dumps more rainwater on an area than the ground can absorb in a short period of time. Floods can also occur when dams are breached. Large waves caused by seismic activity, or *tsunamis*, combine the awesome power and weight of water with flooding, as we saw during the December 26, 2004, tsunami disaster in the South Pacific and Indian Oceans. This tsunami amply demonstrated the enormous destructive capabilities of water and the havoc it can wreak on various businesses and economies.

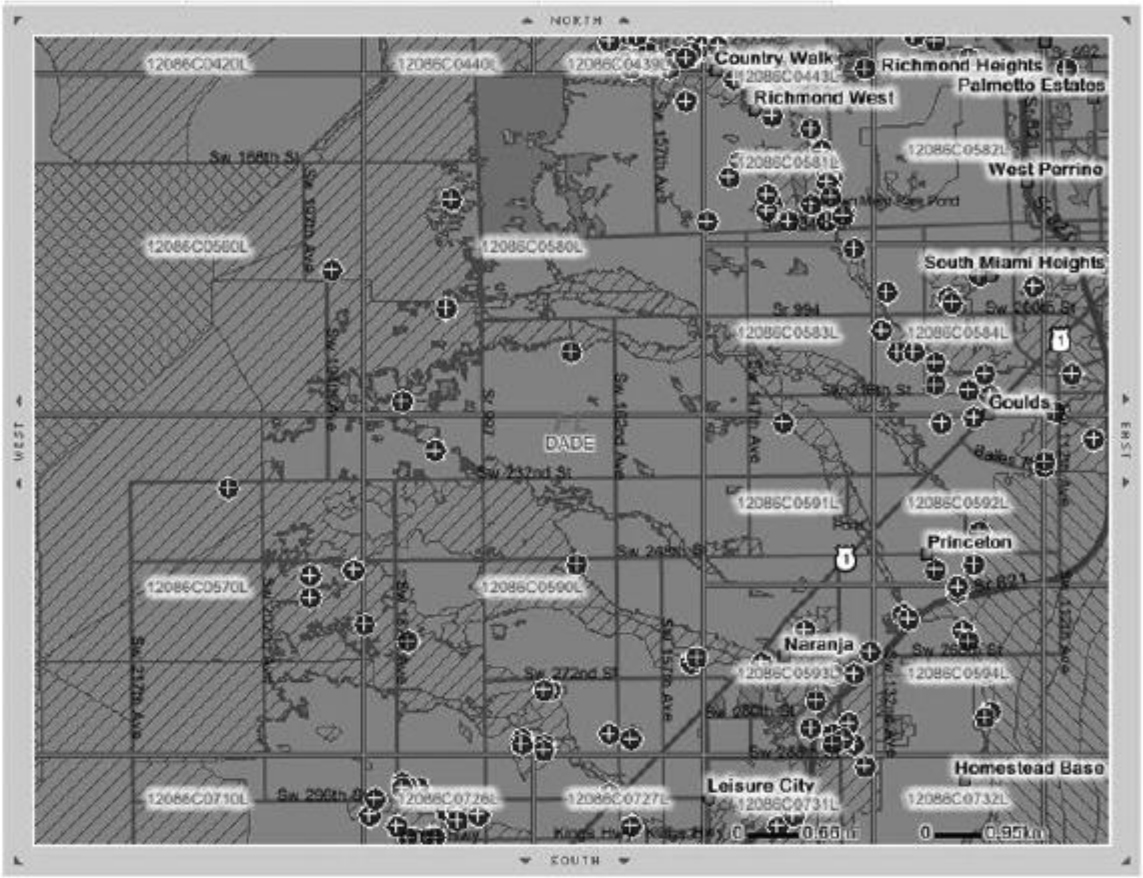
According to government statistics, flooding is responsible for more than $1 billion (that's billion with a *b*!) in damage to businesses and homes each year in the United States. It's important that your DRP make appropriate response plans for the eventuality that a flood may strike your facilities.

> WARNING
>
> When you evaluate a firm's risk of damage from flooding to develop business continuity and disaster recovery plans, it's also a good idea to check with responsible individuals and ensure that your organization has sufficient insurance in place to protect it from the financial impact of a flood. In the United States, most general business policies do not cover flood damage, and you should investigate obtaining specialized government-backed flood insurance under FEMA's National Flood Insurance Program.

Although flooding is theoretically possible in almost any region of the world, it is much more likely to occur in certain areas. FEMA's National Flood Insurance Program is responsible for completing a flood risk assessment for the entire United States and providing this data to citizens in graphical form. You can view flood maps online at www.esri.com/hazards/. This site also provides valuable information on recorded earthquakes, hurricanes, windstorms, hailstorms, and other natural disasters to help you prepare your organization's risk assessment.

When viewing flood maps, like the one shown in Figure 16.1, you'll find that the two risks often assigned to an area are the "100-year flood plain" and the "500-year flood plain." These evaluations mean that the government estimates chances of flooding in any given year at 1 in 100 or at 1 in 500, respectively. For a more detailed tutorial on reading flood maps, visit www.fema.gov/media/fhm/firm/ot_firm.htm.

FIGURE 16.1 Flood hazard map for Miami–Dade County, Florida



Storms

Storms come in many forms and pose diverse risks to a business. Prolonged periods of intense rainfall bring the risk of flash flooding described in the previous section. Hurricanes and tornadoes come with the threat of winds exceeding 100 miles per hour that threaten the structural integrity of buildings and turn everyday objects such as trees, lawn furniture, and even vehicles into deadly missiles. Hailstorms bring a rapid onslaught of destructive ice chunks falling from the sky. Many storms also bring the risk of lightning, which can cause severe damage to sensitive electronic components. For this reason, your business continuity plan should detail appropriate mechanisms to protect against lightning-induced damage, and your disaster recovery plan should provide adequate provisions for power outages and equipment damage that might result from a lightning strike. Never underestimate the damage that a single storm can do.

In 2005, the Category 5 Atlantic hurricane Katrina marked the costliest, deadliest, and strongest hurricane ever to make landfall in the continental

United States. It bored a path of destruction from Alabama to Louisiana, destroying everything natural and man-made throughout those areas. The total economic impact stemming from the damage this storm caused is estimated at upward of $100 billion, eliminating a major Gulf Coast highway and impeding commodities exports, not to mention inundating nearly 80 percent of the city of New Orleans.

> If you live in an area susceptible to a certain type of severe storm, it’s important to regularly monitor weather forecasts from responsible government agencies. For example, disaster recovery specialists in hurricane-prone areas should periodically check the website of the National Weather Service’s Tropical Prediction Center (www.nhc.noaa.gov) during hurricane season. This website allows you to monitor Atlantic and Pacific storms that may pose a risk to your region before word about them hits the local news. This lets you begin a gradual response to the storm before time runs out.

Fires

Fires can start for a variety of reasons, both natural and man made, but both forms can be equally devastating. During the BCP/DRP process, you should evaluate the risk of fire and implement at least basic measures to mitigate that risk and prepare the business for recovery from a catastrophic fire in a critical facility.

Some regions of the world are susceptible to wildfires during the warm season. These fires, once started, spread in somewhat predictable patterns, and fire experts working with meteorologists can produce relatively accurate forecasts of a wildfire’s potential path.

> As with many other types of large-scale natural disasters, you can obtain valuable information about impending threats on the Web. In the United States, the National Interagency Fire Center posts daily fire updates and forecasts on its website: www.nifc.gov/fire_info/maps.htm. Other countries have similar warning systems in place.

Other Regional Events

Some regions of the world are prone to localized types of natural disasters. During the BCP/DRP process, your assessment team should analyze all of your organization's operating locations and gauge the impact that such events might have on your business. For example, many parts of the world are subject to volcanic eruptions. If you conduct operations in an area in close proximity to an active or dormant volcano, your DRP should probably address this eventuality. Other localized natural occurrences include monsoons in Asia, tsunamis in the South Pacific, avalanches in mountainous regions, and mudslides in the western United States.

If your business is geographically diverse, it is prudent to include area natives on your planning team. At the very least, make use of local resources such as government emergency preparedness teams, civil defense organizations, and insurance claim offices to help guide your efforts. These organizations possess a wealth of knowledge and are usually more than happy to help you prepare your organization for the unexpected—after all, every organization that successfully weathers a natural disaster is one less organization that requires a portion of their valuable recovery resources after disaster strikes.

Man-Made Disasters

Our advanced civilization has become increasingly dependent upon complex interactions between technological, logistical, and natural systems. The same complex interactions that make our sophisticated society possible also present a number of potential vulnerabilities from both intentional and unintentional *man-made disasters*. In the following sections, we'll examine a few of the more common disasters to help you analyze your organization's vulnerabilities when preparing a business continuity plan and disaster recovery plan.

Fires

Earlier in the chapter, we explained how some regions of the world are susceptible to wildfires during the warm season, and these types of fires can be described as natural disasters. Many smaller-scale fires result from human action—be it carelessness, faulty electrical wiring, improper fire protection practices, or other reasons. Studies from the Insurance Information Institute indicate that there are at least 1,000 building fires in the United States *every day*. If such a fire strikes your organization, do you have the proper preventative measures in place to quickly contain it? If the fire destroys your facilities, how quickly does your disaster recovery plan allow you to resume operations elsewhere?

Acts of Terrorism

Since the terrorist attacks on September 11, 2001, businesses are increasingly concerned about risks posed by terrorist threats. The attacks on September 11 caused many small businesses to fail because they did not have business continuity/disaster recovery plans in place that were adequate to ensure their continued viability. Many larger businesses experienced significant losses that caused severe long-term damage. The Insurance Information Institute issued a study one year after the attacks that estimated the total damage from the attacks in New York City at $40 billion (yes, that's with a *b*again!).

WARNING

General business insurance may not properly cover an organization against acts of terrorism. Prior to the September 11, 2001, attacks, most policies either covered acts of terrorism or didn't mention them explicitly. After suffering such a catastrophic loss, many insurance companies responded by amending policies to exclude losses from terrorist activity. Policy riders and endorsements are sometimes available but often at extremely high cost. If your business continuity or disaster recovery plan includes insurance as a means of financial recovery (as it probably should!), you'd be well advised to check your policies and contact your insurance professionals to ensure that you're still covered.

Terrorist acts pose a unique challenge to DRP teams because of their unpredictable nature. Prior to the September 11, 2001, terrorist attacks in New York and Washington, D.C., few DRP teams considered the threat of an airplane crashing into their corporate headquarters significant enough to merit mitigation. Many companies are now asking themselves a number of new “what if” questions regarding terrorist activity. In general, these questions are healthy because they promote dialog between business elements regarding potential threats. On the other hand, disaster recovery planners must emphasize solid risk-management principles and ensure that resources aren’t over-allocated to terrorist threats to the detriment of other DRP/BCP activities that protect against more likely threats.

Bombings/Explosions

Explosions can result from a variety of man-made occurrences. Explosive gases from leaks might fill a room/building and later ignite and cause a damaging blast. In many areas, bombings are also cause for concern. From a disaster planning perspective, the effects of bombings and explosions are like those caused by a large-scale fire. However, planning to avoid the impact of a bombing is much more difficult and relies on physical security measures we cover in Chapter 19, “Physical Security Requirements.”

Power Outages

Even the most basic disaster recovery plan contains provisions to deal with the threat of a short power outage. Critical business systems are often protected by uninterruptible power supply (UPS) devices to keep them running at least long enough to shut down or long enough to get emergency generators up and working. Even so, could your organization keep operating during a sustained power outage?

After Hurricane Katrina made landfall in 2005, a reported 900,000 people in Mississippi lost power, with another 600,000 in Alabama. Does your business continuity plan include provisions to keep your business viable during such a prolonged period without power? Does your disaster recovery plan make ample preparations for the timely restoration of power even if the commercial power grid remains unavailable?

WARNING

> Check your UPSs regularly! These critical devices are often overlooked until they become necessary. Many UPSs contain self-testing mechanisms that report problems automatically, but it’s still a good idea to subject them to regular testing. Also, be sure to audit the number/type

of devices plugged in to each UPS. It’s amazing how many people think it’s okay to add “just one more system” to a UPS, and you don’t want to be surprised when the device can’t handle the load during a real power outage!

Today’s technology-driven organizations depend increasingly on electric power, so your BCP/DRP team should consider provisioning alternative power sources that can run business systems indefinitely. An adequate backup generator could make a huge difference when the survival of your business is at stake.

Other Utility and Infrastructure Failures

When planners consider the impact that utility outages may have on their organizations, they naturally think first about the impact of a power outage. However, keep other utilities in mind too. Do any of your critical business systems rely on water, sewers, natural gas, or other utilities? Also consider regional infrastructure such as highways, airports, and railroads. Any of these systems can suffer failures that might not be related to weather or other conditions described in this chapter. Many businesses depend on one or more of these infrastructure elements to move people or materials. Their failure can paralyze your business’s ability to continue functioning.

NOTE

If you quickly answered no when asked whether you have critical business systems that rely on water, sewers, natural gas, or other utilities, think again. Do you consider people a critical business system? If a major storm knocks out the water supply to your facilities and you need to keep those facilities up and running, can you supply your employees with enough drinking water to meet their needs?

What about your fire protection systems? If any of them are water based, is there a holding tank system in place that contains ample water to extinguish a serious building fire if the public water system is unavailable? Fires often cause serious damage in areas ravaged by storms, earthquakes, and other disasters that might also interrupt the delivery of water.

Hardware/Software Failures

Like it or not, computer systems fail. Hardware components simply wear out and refuse to continue performing, or they suffer physical damage. Software systems contain bugs or fall prey to improper or unexpected inputs. For this reason, BCP/DRP teams must provide adequate redundancy in their systems. If zero downtime is a mandatory requirement, the best solution is to use fully redundant failover servers in separate locations attached to separate communications links and infrastructures (also designed to operate in a failover mode). If one server is damaged or destroyed, the other will instantly take over the processing load. For more information on this concept, see the section “Remote Mirroring” later in this chapter.

Because of financial constraints, it isn’t always feasible to maintain fully redundant systems. In those circumstances, the BCP/DRP team should address how replacement parts can be quickly obtained and installed. As many parts as possible should be kept in a local parts inventory for quick replacement; this is especially true for hard-to-find parts that must otherwise be shipped in. After all, how many organizations could do without telephones for three days while a critical PBX component is en route from an overseas location to be installed on site?

NYC Blackout

On August 14, 2003, the lights went out in New York City and in large areas of the northeastern and midwestern United States when a series of cascading failures caused the collapse of a major power grid.

Fortunately, security professionals in the New York area were ready. Spurred to action by the September 11, 2001, terrorist attacks, many businesses updated their disaster recovery plans and took steps to ensure their continued operations in the wake of another disaster. This blackout served to test those plans, and many organizations were able to continue operating on alternate power sources or transferred control seamlessly to offsite data-processing centers.

Lessons learned during this blackout offer insight for BCP/DRP teams around the world:

- Ensure that alternate processing sites are far enough away from your main site that they are unlikely to be affected by the same disaster.
- Remember that threats to your organization are both internal and external. Your next disaster may come from a terrorist attack, building fire, or malicious code running loose on your network. Take steps to ensure that your alternate sites are segregated from the main facility to protect against all of these threats.
- Disasters don't usually come with advance warning. If real-time operations are critical to your organization, be sure that your backup sites are ready to assume primary status at a moment's notice.

Strikes/Picketing

When designing your business continuity and disaster recovery plans, don't forget about the importance of the human factor in emergency planning. One form of man-made disaster that is often overlooked is the possibility of a strike or other labor crisis. If a large number of your employees walk out at the same time, what impact would that have on your business? How long would you be able to sustain operations without the regular full-time employees that staff a certain area? Your BCP and DRP teams should address these concerns, providing alternative plans should a labor crisis occur.

Theft/Vandalism

In a previous section, we talked about the threat that terrorist activities pose to an organization. Theft and vandalism represent the same kind of threat on a much smaller scale. In most cases, however, there's a far greater chance that your organization will be affected by theft or vandalism than by a terrorist attack. Insurance provides some financial protection against these events (subject to deductibles and limitations of coverage), but acts of this kind can cause serious damage to your business, on both a short-term and long-term basis. Your business continuity and disaster recovery plans should include adequate preventive measures to control the frequency of these occurrences as well as contingency plans to mitigate the effects theft and vandalism have on ongoing operations.

Offsite Challenges to Security

The constant threat of theft and vandalism is the bane of information security professionals worldwide. Personal identity information, proprietary or trade secrets, and other forms of confidential data are just as interesting to those who create and possess them as they are to direct competitors and other unauthorized parties.

Aaron knows this first-hand working as a security officer for a very prominent and highly visible computing enterprise. His chief responsibility is to keep sensitive information from exposure to various elements and entities. Bethany is one of his more troublesome employees because she’s constantly taking her notebook computer off site without properly securing its contents.

Even a casual smash-and-grab theft attempt could put thousands of client contacts and their confidential business dealings at risk of being leaked and possibly sold to malicious parties. Aaron knows the potential dangers, but Bethany just doesn’t seem to care.

This poses the question, How might you better inform, train, or advise Bethany so that Aaron does not have to relieve her of her position should her notebook be stolen? Bethany must come to understand and appreciate the importance of keeping sensitive information secure. It may be necessary to emphasize the potential loss and exposure that comes with losing such data to wrongdoers, competitors, or other unauthorized third parties. It may suffice to point out to Bethany that the employee handbook clearly states that employees whose behavior leads to the unauthorized disclosure or loss of information assets are subject to loss of pay or termination. If such behavior recurs after a warning, Bethany should be rebuked and reassigned to a position where she can’t expose sensitive or proprietary information, that is, if she’s not fired on the spot.

NOTE

Keep the impact that theft may have on your operations in mind when planning your parts inventory. It’s a good idea to keep extra inventory of items with a high pilferage rate, such as RAM chips and laptops. It’s also a good idea to keep such materials in secure storage and to require employees to sign such items out whenever they are used.

Recovery Strategy

When a disaster interrupts your business, your disaster recovery plan should kick in nearly automatically and begin providing support for recovery operations. The disaster recovery plan should be designed so that the first employees on the scene can immediately begin the recovery effort in an organized fashion, even if members of the official DRP team have not yet arrived on site. In the following sections, we’ll cover critical subtasks involved in crafting an effective disaster recovery plan that can guide rapid restoration of regular business processes and resumption of activity at the primary business location.

In addition to improving your response capabilities, purchasing insurance can reduce the risk of financial losses. When selecting insurance, be sure to purchase sufficient coverage to enable you to recover from a disaster. Simple value coverage may be insufficient to encompass actual replacement costs. If your property insurance includes an actual cash value (ACV) clause, then your damaged property will be compensated based on the fair market value of the items on the date of loss less all accumulated depreciation since the time of their purchase. The important point here is that unless you have a replacement cost clause in your insurance coverage, your organization is likely to be out of pocket as a result of any losses it might sustain.

Valuable paper insurance coverage provides protection for inscribed, printed, and written documents and manuscripts and other printed business records. However, it does not cover damage to paper money and printed security certificates.

Business Unit and Functional Priorities

To recover your business operations with the greatest possible efficiency, you must engineer your disaster recovery plan so that those business units with the highest priority are recovered first. You must identify and prioritize critical business functions as well so you can define which functions to restore after a disaster or failure and in what order.

To achieve this goal, the DRP team must first identify those business units and agree on an order of prioritization, and they must do likewise with business functions. (And take note: Not all critical business functions will necessarily be carried out in critical business units, so the final results of this analysis will very probably comprise a superset of critical business units plus other select units.)

If this process sounds familiar, it should! This is very like the prioritization task the BCP team performs during the business impact assessment discussed in the previous chapter. In fact, most organizations will complete a business impact analysis (BIA) as part of their business continuity planning process. This analysis identifies vulnerabilities, develops strategies to minimize risk, and ultimately produces a BIA report that describes the potential risks that an organization faces and identifies critical business units and functions. A BIA also identifies costs related to failures that include loss of cash flow, equipment replacement, salaries paid to clear work backlogs, profit losses, opportunity costs from the inability to attract new business, and so forth. Such failures are assessed in terms of potential impacts on finances, personnel, safety, legal compliance, contract fulfillment, and quality assurance, preferably in monetary terms to make impacts comparable and to set budgetary expectations. With all this BIA information in hand, you should use the resulting documentation as the basis for this prioritization task.

At a minimum, the output from this task should be a simple listing of business units in priority order. However, a more detailed list, broken down into specific business processes listed in order of priority, would be a much more useful deliverable. This business-process-oriented list is more reflective of real-world conditions, but it requires considerable additional effort. It will, however, greatly assist in the recovery effort—after all, not every task performed by the highest-priority business unit will be of the highest priority. You might find that it would be best to restore the highest-priority unit to 50 percent capacity and then move on to lower-priority units to achieve some minimum operating capacity across the organization before attempting a full recovery effort.

By the same token, the same exercise must be completed for critical business processes and functions. Not only can these things involve multiple business units and cross the lines between them, they define the operational elements that must be restored in the wake of a disaster or other business interruption. Here also, the final result should be a checklist of items in priority order, each with its own risk and cost assessment, and a corresponding set of mean time to recovery (MTR) and related recovery objectives and milestones.

Crisis Management

If a disaster strikes your organization, panic is likely to set in. The best way to combat this is with an organized disaster recovery plan. The individuals in your business who are most likely to first notice an emergency situation (that is, security guards, technical personnel, and so on) should be fully trained in disaster recovery procedures and know the proper notification procedures and immediate response mechanisms.

Many things that normally seem like common sense (such as calling 911 in the event of a fire) may slip the minds of panicked employees seeking to flee an emergency. The best way to combat this is with continuous training on disaster recovery responsibilities. Returning to the fire example, all employees should be trained to activate the fire alarm or contact emergency officials when they spot a fire (after, of course, taking appropriate measures to protect themselves). After all, it’s better that the fire department receives 10 different phone calls reporting a fire at your organization than it is for everyone to assume that someone else already took care of it.

Crisis management is a science and an art form. If your training budget permits, investing in crisis training for your key employees is a good idea. This ensures that at least some of your employees know how to handle emergency situations properly and can provide all-important “on-the-scene” leadership to panic-stricken co-workers.

Emergency Communications

When a disaster strikes, it is important that the organization be able to communicate internally as well as with the outside world. A disaster of any significance is easily noticed, but if an organization is unable to keep the outside world informed of its recovery status, the public is apt to fear the worst and assume that the organization is unable to recover. It is also essential that the organization be able to communicate internally during a disaster so that employees know what is expected of them—whether they are to return to work or report to another location, for instance.

In some cases, the circumstances that brought about the disaster to begin with may have also damaged some or all normal means of communications. A violent storm or an earthquake may have also knocked out telecommunications systems; at that point it's too late to try to figure out other means of communicating both internally and externally.

Work Group Recovery

When designing a disaster recovery plan, it's important to keep your goal in mind—the restoration of work groups to the point that they can resume their activities in their usual work locations. It's very easy to get sidetracked and think of disaster recovery as purely an IT effort focused on restoring systems and processes to working order.

To facilitate this effort, it's sometimes best to develop separate recovery facilities for different work groups. For example, if you have several subsidiary organizations that are in different locations and that perform tasks similar to the tasks that work groups at your office perform, you may want to consider temporarily relocating those work groups to the other facility and having them communicate electronically and via telephone with other business units until they're ready to return to the main operations facility.

Larger organizations may have difficulty finding recovery facilities capable of handling the entire business operation. This is another example of a circumstance in which independent recovery of different work groups is appropriate.

Alternate Processing Sites

One of the most important elements of the disaster recovery plan is the selection of alternate processing sites to be used when the primary sites are unavailable. Many options are available when considering recovery facilities, limited only by the creative minds of disaster recovery planners and service providers. In the following sections, we cover several types of sites commonly used in disaster recovery planning: cold sites, warm sites, hot sites, mobile sites, service bureaus, and multiple sites.

NOTE

When choosing any alternate processing site, be sure to situate it far away enough from your primary location that it won’t be affected by the same disaster that disables your primary site.

Cold Sites

Cold sites are simply standby facilities large enough to handle the processing load of an organization and equipped with appropriate electrical and environmental support systems. They may be large warehouses, empty office buildings, or other similar structures. However, a cold site has no computing facilities (hardware or software) preinstalled with no active broadband communications links. Many cold sites do have at least a few copper telephone lines, and some sites may have standby links that can be activated with minimal notification.

Cold Site Setup

A cold site setup is best depicted in the fictional work *Boiler Room*, which involves a chop-shop investment firm telemarketing bogus pharmaceutical investment deals to prospective clients. In this fictional case, the “disaster” is man made, but the concept is much the same, even if the timing is quite different.

Under threat of exposure and a pending law enforcement raid, the firm establishes a nearby building that is empty, save for a few banks of phones on dusty concrete floors in a mock-up of a cold recovery site. Granted, this work is both fictional and illegal, but it illustrates a

> very real and legitimate reason for maintaining a redundant fail-over recovery site for the purpose of business continuity.
>
> Research the various forms of recovery sites, and then consider which among them is best suited for your particular business needs and budget. A cold site is the least expensive option and perhaps the most practical. A warm site contains the data links and preconfigured equipment necessary to begin restoring operations but no usable data or information. The most expensive option is a hot site, which fully replicates your existing business infrastructure and is ready to take over for the primary site on short notice.

The major advantage of a cold site is its relatively low cost—there's no computing base to maintain and no monthly telecommunications bill when the site is idle. However, the drawbacks of such a site are obvious—there is a tremendous lag time between the time the decision is made to activate the site and the time when that site is actually ready to support business operations. Servers and workstations must be brought in and configured. Data must be restored from backup tapes. Communications links must be activated or established. The time to activate a cold site is often measured in weeks, making timely recovery close to impossible and often yielding a false sense of security. It's also worth observing that the substantial time, effort, and expense required to activate and transfer operations to a cold site make this approach the most difficult to test.

Hot Sites

A *hot site* is the exact opposite of the cold site. In this configuration, a backup facility is maintained in constant working order, with a full complement of servers, workstations, and communications links ready to assume primary operations responsibilities. The servers and workstations are all preconfigured and loaded with appropriate operating system and application software.

> TIP

When choosing a facility, be sure it is far enough away from the original site so as not to be affected by the same disaster yet close enough that it doesn’t take a full day’s drive to reach it.

The data on the primary site servers is periodically or continuously replicated to corresponding servers at the hot site, ensuring that the hot site has up-to-date data. Depending on the bandwidth available between the sites, hot site data may be replicated instantaneously. If that is the case, operators could simply move operations to the hot site at a moment’s notice. If it’s not the case, disaster recovery managers have three options to activate the hot site:

- If there is sufficient time before the primary site must be shut down, they can force replication between the two sites right before the transition of operational control.
- If replication is impossible, managers may carry backup tapes of the transaction logs from the primary site to the hot site and manually reapply any transactions that took place since the last replication.
- If there are no available backups and it isn’t possible to force replication, the disaster recovery team may simply accept the loss of some portion of the data.

The advantages of a hot site are obvious—the level of disaster recovery protection provided by this type of site is unsurpassed. However, the cost is *extremely* high. Maintaining a hot site essentially doubles an organization’s budget for hardware, software, and services and requires the use of additional employees to maintain the site.

WARNING

If you use a hot site, never forget that it has copies of your production data. Be sure to provide that site with the same level of technical and physical security controls you provide at your primary site.

If an organization wants to maintain a hot site but wants to reduce the expense of equipment and maintenance, it might opt to use a shared hot site facility managed by an outside contractor. However, the inherent danger in these facilities is that they may be overtaxed in the event of a widespread disaster and be unable to service all clients simultaneously. If your organization considers such an arrangement, be sure to investigate these issues thoroughly, both before signing the contract and periodically during the contract term.

Warm Sites

Warm sites occupy the middle ground between hot and cold sites for disaster recovery specialists. They always contain the equipment and data circuits necessary to rapidly establish operations. As it is in hot sites, this equipment is usually preconfigured and ready to run appropriate applications to support an organization's operations. Unlike hot sites, however, warm sites do not typically contain copies of the client's data. The main requirement in bringing a warm site to full operational status is the transportation of appropriate backup media to the site and restoration of critical data on the standby servers.

Activation of a warm site typically takes at least 12 hours from the time a disaster is declared. This does not mean that any site that can be activated in less than 12 hours qualifies as a hot site, however: Switchover times for most hot sites are often measured in seconds or minutes, and complete cutovers seldom take more than an hour or two.

However, warm sites avoid significant telecommunications and personnel costs inherent in maintaining a near-real-time copy of the operational data environment. As with hot sites and cold sites, warm sites may also be obtained on a shared facility basis. If you choose this option, be sure that you have a "no lockout" policy written into your contract guaranteeing you the use of an appropriate facility even during a period of high demand. It's a good idea to take this concept one step further and physically inspect the facilities and the contractor's operational plan to reassure yourself that the facility will indeed be able to back up the "no lockout" guarantee should push ever come to shove.

Mobile Sites

Mobile sites are nonmainstream alternatives to traditional recovery sites. They typically consist of self-contained trailers or other easily relocated units. These sites include all the environmental control systems necessary to maintain a safe computing environment. Larger corporations sometimes maintain these sites on a "fly-away" basis, ready to deploy them to any operating location around the world via air, rail, sea, or surface transportation. Smaller firms might contract with a mobile site vendor in their local area to provide these services on an as-needed basis.

> If your disaster recovery plan depends on a workgroup recovery strategy, mobile sites are an excellent way to implement that approach. They are often large enough to accommodate entire (small!) work groups.

Mobile sites are often configured as cold sites or warm sites, depending upon the disaster recovery plan they are designed to support. It is also possible to configure a mobile site as a hot site, but this is unusual because one seldom knows in advance where a mobile site will be deployed.

Hardware Replacement Options

One thing to consider when determining mobile sites and recovery sites in general is hardware replacement supplies. There are basically two options for hardware replacement supplies. One option is to employ “in-house” replacement whereby you store extra and duplicate equipment at a different but nearby location (that is, a warehouse on the other side of town). (*In-house* here means you own it already, not that it is necessarily housed under the same roof as your production environment.) If you have a hardware failure or a disaster, you can immediately pull the appropriate equipment from your stash. The other option is an SLA-type agreement with a vendor to provide quick response and delivery time in the event of a disaster. However, even a 4-, 12-, 24-, or 48-hour replacement hardware contract from a vendor does not provide a reliable guarantee that delivery will actually occur. There are too many uncontrollable variables to rely upon this second option as your sole means of recovery.

Service Bureaus

A *service bureau* is a company that leases computer time. Service bureaus own large server farms and often fields of workstations. Any organization can purchase a contract from a service bureau to consume some portion of their processing capacity. Access can be on site or remote.

A service bureau can usually provide support for all your IT needs in the event of a disaster, even desktops for workers to use. Your contract with a service bureau will often include testing and backups as well as response time and availability. However, service bureaus regularly oversell their actual capacity by gambling that not all their contracts will be exercised at the same time. Therefore, there is potential for resource contention in the wake of a major disaster. If your company operates in an industry-dense locale, this could be an important issue. You may need to select both a local and a distant service bureau to be sure to gain access to processing facilities during a real disaster.

Multiple Sites

By splitting or dividing your outfit into several divisions, branches, offices, and so on, you create multiple sites and reduce the impact of a major disaster. In fact, the more sites you employ, the less impact a major disaster will have. However, for multiple sites to be effective, they must be far enough apart that a major disaster cannot affect too many of them simultaneously. One drawback of using multiple sites is that it increases the difficulty of managing and administering the entire company when it’s spread across a large geographic area in numerous locations.

Mutual Assistance Agreements

Mutual assistance agreements (MAAs), also called *reciprocal agreements*, are popular in disaster recovery literature but are rarely implemented in real-world practice. In theory, they provide an excellent alternate processing option. Under an MAA, two organizations pledge to assist each other in the event of a disaster by sharing computing facilities or other technological resources. They appear to be extremely cost effective at first glance—it’s not necessary for either organization to maintain expensive alternate processing sites (such as the hot sites, warm sites, cold sites, and mobile processing sites described in the previous sections). Indeed, many

MAAs are structured to provide one of the levels of service described. In the case of a cold site, each organization may simply maintain some open space in their processing facilities for the other organization to use in the event of a disaster. In the case of a hot site, the organizations may host fully redundant servers for each other.

However, many drawbacks inherent to MAAs prevent their widespread use:

- MAAs are difficult to enforce. The parties trust each other to provide support in the event of a disaster. However, when push comes to shove, the nonvictim might renege on the agreement. A victim may have legal remedies available, but this doesn't help the immediate disaster recovery effort.
- Cooperating organizations should be located in relatively close proximity to each other to facilitate transportation of employees between sites. However, proximity means that both organizations may be vulnerable to the same threats. An MAA won't do you any good if an earthquake levels your city and destroys processing sites for *both* participating organizations.
- Confidentiality concerns often prevent businesses from placing their data in the hands of others. These may be legal concerns (such as in the handling of health-care or financial data) or business concerns (such as trade secrets or other intellectual property issues).

Despite these concerns, an MAA may be a good disaster recovery solution for an organization, especially if cost is an overriding factor. If you simply can't afford to implement any other type of alternate processing, an MAA might provide a degree of valuable protection in the event a localized disaster strikes your business.

Database Recovery

Many organizations rely upon databases to process and track operations, sales, logistics, and other activities vital to their continued viability. For this reason, it's essential that you include database recovery techniques in your disaster recovery plans. It's a wise idea to have a database specialist on the DRP team who can provide input as to the technical feasibility of various ideas. After all, you shouldn't allocate several hours to restore a database backup when it's impossible to complete a restoration in less than half a day!

In the following sections, we'll cover the three main techniques used to create offsite copies of database content: electronic vaulting, remote journaling, and remote mirroring. Each one has specific benefits and drawbacks, so you’ll need to analyze your organization’s computing requirements and available resources to select the option best suited to your firm.

Electronic Vaulting

In an *electronic vaulting* scenario, database backups are transferred to a remote site using bulk transfers. The remote location may be a dedicated alternative recovery site (such as a hot site) or simply an offsite location managed within the company or by a contractor for the purpose of maintaining backup data. If you use electronic vaulting, remember that there may be a significant time delay between the time you declare a disaster and the time your database is ready for operation with current data. If you decide to activate a recovery site, technicians will need to retrieve the appropriate backups from the electronic vault and apply them to the soon-to-be production servers at the recovery site.

> WARNING
>
> Be careful when considering vendors for an electronic vaulting contract. Definitions of electronic vaulting vary widely within the industry. Don’t settle for a vague promise of “electronic vaulting capability.” Insist upon a written definition of the service that will be provided, including the storage capacity, bandwidth of the communications link to the electronic vault, and the time necessary to retrieve vaulted data in the event of a disaster.

As with any type of backup scenario, be certain to periodically test your electronic vaulting setup. A great method for testing backup solutions is to give disaster recovery personnel a “surprise test,” asking them to restore data from a certain day.

Remote Journaling

With *remote journaling*, data transfers are performed in a more expeditious manner. Data transfers still occur in a bulk transfer mode, but they occur on a more frequent basis, usually once every hour if not more frequently. Unlike electronic vaulting scenarios, where database backup files are transferred, remote journaling setups transfer copies of the database transaction logs containing the transactions that occurred since the previous bulk transfer.

Remote journaling is similar to electronic vaulting in that transaction logs transferred to the remote site are not applied to a live database server but are maintained in a backup device. When a disaster is declared, technicians retrieve the appropriate transaction logs and apply them to the production database.

Remote Mirroring

Remote mirroring is the most advanced database backup solution. Not surprisingly, it's also the most expensive! Remote mirroring goes beyond the technology used by remote journaling and electronic vaulting; with remote mirroring, a live database server is maintained at the backup site. The remote server receives copies of the database modifications at the same time they are applied to the production server at the primary site. Therefore, the mirrored server is ready to take over an operational role at a moment's notice.

Remote mirroring is a popular database backup strategy for organizations seeking to implement a hot site. However, when weighing the feasibility of a remote mirroring solution, be sure to take into account the infrastructure and personnel costs required to support the mirrored server as well as the processing overhead that will be added to each database transaction on the mirrored server.

Recovery Plan Development

Once you've established your business unit priorities and have a good idea of the appropriate alternative recovery sites for your organization, it's time to put pen to paper and begin drafting a true disaster recovery plan. Don't expect to sit down and write the full plan in one sitting. It's likely that the DRP team will go through many evolutions of draft documents before reaching a final written document that satisfies the operational needs of critical business units and falls within the resource, time, and expense constraints of the disaster recovery budget and available manpower.

In the following sections, we explore some important items to include in your disaster recovery plan. Depending on the size of your organization and the number of people involved in the DRP effort, it may be a good idea to maintain multiple types of plan documents, intended for different audiences. The following list includes various types of documents worth considering:

- Executive summary
- Department-specific plans
- Technical guides for IT personnel responsible for implementing and maintaining critical backup systems
- Checklists for individuals on the disaster recovery team
- Full copies of the plan for critical disaster recovery team members

Using custom-tailored documents becomes especially important when a disaster occurs or is imminent. Personnel who need to refresh themselves on the disaster recovery procedures that affect various parts of the organization will be able to refer to their department-specific plans. Critical disaster recovery team members will have checklists to help guide their actions amid the chaotic atmosphere of a disaster. IT personnel will have technical guides helping them get the alternate sites up and running. Finally, managers and public relations personnel will have a simple document that walks them through a high-level view of the coordinated symphony that is an active disaster recovery effort without requiring interpretation from team members busy with tasks directly related to that effort.

TIP

Visit the Professional Practices library at www.drii.org/professionalprac/ to examine a collection of documents that explain how to work through and document your planning processes for BCP and disaster recovery. Other good standard documents in this area includes the BCI Good Practices Guideline (www.thebci.org/gpg/htm), ISO 27001 (www.27001-online.com), and NIST SP 800-34 (http://csrc.nist.gov/publications/PubsSPs.html).

Emergency Response

A disaster recovery plan should contain simple yet comprehensive instructions for essential personnel to follow immediately upon recognizing that a disaster is in progress or is imminent. These instructions will vary widely depending upon the nature of the disaster, the type of personnel responding to the incident, and the time available before facilities need to be evacuated and/or equipment shut down. For example, instructions for a large-scale fire will be much more concise than the instructions for how to prepare for a hurricane that is still 48 hours away from a predicted landfall near an operational site. Emergency-response plans are often put together in the form of checklists provided to responders. When designing such checklists, keep one essential design principle in mind: Arrange the checklist tasks in order of priority, with the most important task first!

It's essential to remember that these checklists will be executed in the midst of a crisis. It is extremely likely that responders will not be able to complete the entire checklist, especially in the event of a short-notice disaster. For this reason, you should put the most essential tasks (that is, "Activate the building alarm") first on the checklist. The lower an item on the list, the lower the likelihood that it will be completed before an evacuation/shutdown takes place.

Personnel Notification

A disaster recovery plan should also contain a list of personnel to contact in the event of a disaster. Usually, this includes key members of the DRP team as well as personnel who execute critical disaster recovery tasks throughout the organization. This response checklist should include alternate means of contact (that is, pager numbers, cell phone numbers, and so on) as well as backup contacts for each role should the primary contact be incommunicado or unable to reach the recovery site for one reason or another.

The Power of Checklists

Checklists are invaluable tools in the face of disaster. They provide a sense of order amidst the chaotic events surrounding a disaster. Do what you must to ensure that response checklists provide first responders with a clear plan to protect life and property and ensure the continuity of operations.

A checklist for response to a building fire might include the following steps:

1. Activate the building alarm system.

2. Ensure that an orderly evacuation is in progress.

3. After leaving the building, use a cellular telephone to call 911 to ensure that emergency authorities received the alarm notification. Provide additional information on any required emergency response.

4. Ensure that any injured personnel receive appropriate medical treatment.

5. Activate the organization's disaster recovery plan to ensure continuity of operations.

Be sure to consult with the individuals in your organization responsible for privacy before assembling and disseminating a telephone notification checklist. You may need to comply with special policies regarding the use of home telephone numbers and other personal information in the checklist.

The notification checklist should be supplied to all personnel who might respond to a disaster. This enables prompt notification of key personnel. Many firms organize their notification checklists in a "telephone tree" style: Each member of the tree contacts the person below them, spreading the notification burden among members of the team instead of relying on one person to make lots of telephone calls.

TIP

If you choose to implement a telephone tree notification scheme, be sure to add a safety net. Have the last person in each chain contact the originator to confirm that their entire chain has been notified. This lets you rest assured that the disaster recovery team activation is smoothly underway.

Backups and Offsite Storage

Your disaster recovery plan (especially the technical guide) should fully address the backup strategy pursued by your organization. Indeed, this is one of the most important elements of any business continuity plan and disaster recovery plan.

Many system administrators are already familiar with various types of backups, so you'll benefit by bringing one or more individuals with specific technical expertise in this area onto the BCP/DRP team to provide expert guidance. There are three main types of backups:

Full backups As the name implies, *full backups* store a complete copy of the data contained on the protected device. Full backups duplicate every file on the system regardless of the setting of the archive bit. Once a full backup is complete, the archive bit on every file is reset, turned off, or set to 0.

Incremental backups *Incremental backups* store only those files that have been modified since the time of the most recent full or incremental backup. Only files that have the archive bit turned on, enabled, or set to 1 are duplicated. Once an incremental backup is complete, the archive bit on all duplicated files is reset, turned off, or set to 0.

Differential backups *Differential backups* store all files that have been modified since the time of the most recent full backup. Only files that have the archive bit turned on, enabled, or set to 1 are duplicated. However, unlike full and incremental backups, the differential backup process does not change the archive bit.

The most important difference between incremental and differential backups is the time needed to restore data in the event of an emergency. If you use a combination of full and differential backups, you will need to restore only two backups—the most recent full backup and the most recent differential backup. On the other hand, if your strategy combines full backups with incremental backups, you will need to restore the most recent full backup as well as all incremental backups performed since that full backup. The trade-off is the time required to *create* the backups—differential backups don't take as long to restore, but they take longer to create than incremental ones.

The storage of the backup media is equally critical. It may be convenient to store backup media in or near the primary operations center to easily fulfill user requests for backup data, but you'll definitely need to keep copies of the media in at least one offsite location to provide redundancy should your primary operating location be suddenly destroyed.

Using Backups

In case of system failure, many companies use one of two common methods to restore data from backups. In the first situation, they run a full backup on Monday night and then run differential backups every other night of the week. If a failure occurs Saturday morning, they restore Monday's full backup and then restore only Friday's differential backup. In the second situation, they run a full backup on Monday night and run incremental backups every other night of the week. If a failure occurs Saturday morning, they restore Monday's full backup and then restore each incremental backup in original chronological order (that is, Wednesday's, then Friday's, and so on).

Most organizations adopt a backup strategy that utilizes more than one of the three backup types along with a media rotation scheme. Both allow backup administrators access to a sufficiently large range of backups to complete user requests and provide fault tolerance while minimizing the amount of money that must be spent on backup media. A common strategy is to perform full backups over the weekend and incremental or differential backups on a nightly basis. The specific method of backup and all of the particulars of the backup procedure are dependent upon your organization's fault-tolerance requirements. If you are unable to survive minor amounts of data loss, then your ability to tolerate faults is low. However, if hours or days of data can be lost without serious consequence, then your tolerance of faults is high. You should design your backup solution accordingly.

The Oft-Neglected Backup

Backups are probably the least practiced and most neglected preventive measure known to protect against computing disasters. A comprehensive backup of all operating system and personal data on workstations happens less frequently than for servers or mission-critical machines, but they all serve an equal and necessary purpose.

Carol, an information professional, learned this the hard way when she lost months of work following a natural disaster that wiped out the first floor at an information brokering firm. She never utilized the backup facilities built into her operating system or any of the shared provisions established by her administrator, Damon.

Damon has been there and done that, so he knows a thing or two about backup solutions. He has established incremental backups on his production servers and differential backups on his development servers, and he's never had an issue restoring lost data.

The toughest obstacle to a solid backup strategy is human nature, so a simple, transparent, and comprehensive strategy is the most practical. Differential backups require only two container files (the latest full backup and the latest differential) and can be scheduled for periodic updates at some specified interval. That's why Damon elects to implement this approach and feels ready to restore from his backups any time he's called upon to do so.

Backup Media Formats

The physical characteristics and the rotation cycle are two factors that a worthwhile backup solution should track and manage. The physical characteristics involve the type of tape drive in use. This defines the physical wear placed on the media. The rotation cycle is the frequency of backups and retention length of protected data. By overseeing these characteristics, you can be assured that valuable data will be retained on serviceable backup media. Backup media has a maximum use limit; perhaps 5, 10, or 20 rewrites may be made before the media begins to lose reliability (statistically speaking). A wide variety of backup media formats exist:

- Digital Audio Tape (DAT)
- Quarter Inch Cartridge (QIC), commonly used in SOHO backups
- 8 mm tape, commonly used in Helical Scan tape drives but has been superseded by DLT
- Digital Linear Tape (DLT)
- Write Once, Read Many (WORM), a storage type often used to retain audit trails
- CDR/W media, usually requires faster file access than tape, useful for temporary storage of changeable data

There is increasing and widespread use of storage arrays as the backup medium of choice. With drives now 3 TB in size, tape and optical media can't really cope with data volume requirements anymore. Most enterprises use storage area networks (SANs) or network attached storage (NAS) for backup nowadays.

Writeable CDs and DVDs as well as removable drives (Winchester, Zip, Jaz, and so forth) are considered inappropriate for network backup solutions, primarily because of their limited capacity but in some cases because of their speed or buffer underflow problems. Buffer underflow problems occurred before the advent of burn-proof software. *Underflow* happens when the write buffer of the drive empties during the writing process, which causes an error on the media, rendering it useless. However, these types of backup media are appropriate for end users to perform backups of limited sets of data from specific applications or for personal archiving purposes.

Backup Best Practices

No matter what the backup solution, media, or method, you must address several common issues with backups. For instance, backup and restoration activities can be bulky and slow. Such data movement can significantly affect the performance of a network, especially during regular production hours. Thus, backups should be scheduled during the low peak periods (for example, at night).

The amount of backup data increases over time. This causes the backup (and restoration) processes to take longer each time and to consume more space on the backup media. Thus, you need to build sufficient capacity to handle a reasonable amount of growth over a reasonable amount of time into your backup solution. What is reasonable all depends on your environment and budget.

With periodic backups (that is, backups that are run every 24 hours), there is always the potential for data loss up to the length of the period. Murphy's law dictates that a server never crashes immediately after a successful backup. Instead, it is always just before the next backup begins. To avoid the problem with periods, you need to deploy some form of real-time continuous backup, such as RAID, clustering, or server mirroring.

Tape Rotation

There are several commonly used tape rotation strategies for backups: the Grandfather-Father-Son (GFS) strategy, the Tower of Hanoi strategy, and the Six Cartridge Weekly Backup strategy. These strategies can be fairly complex, especially with large tape sets. They can be implemented manually using a pencil and a calendar or automatically by using either commercial backup software or a fully automated hierarchical storage management (HSM) system. An HSM system is an automated robotic backup jukebox consisting of 32 or 64 optical or tape backup devices. All the drive elements within an HSM system are configured as a single drive array (a bit like RAID).

NOTE

Details about various tape rotations are beyond the scope of this book, but if you want to learn more about them, search by their names on the Internet.

Software Escrow Arrangements

A *software escrow arrangement* is a unique tool used to protect a company against the failure of a software developer to provide adequate support for its products or against the possibility that the developer will go out of business and no technical support will be available for the product.

> Focus your efforts on negotiating software escrow agreements with those suppliers you fear may go out of business because of their size. It's not likely that you'll be able to negotiate such an agreement with a firm such as Microsoft, unless you are responsible for an extremely large corporate account with serious bargaining power. On the other hand, it's equally unlikely that a firm of Microsoft's magnitude will go out of business, leaving end users high and dry.

If your organization depends upon custom-developed software or software products produced by a small firm, you may want to consider developing this type of arrangement as part of your disaster recovery plan. Under a software escrow agreement, the developer provides copies of the application source code to an independent third-party organization. This third party then maintains updated backup copies of the source code in a secure fashion. The agreement between the end user and the developer specifies "trigger events," such as the failure of the developer to meet terms of a service-level agreement (SLA) or the liquidation of the developer's firm. When a trigger event takes place, the third party releases copies of the application source code to the end user. The end user can then analyze the source code to resolve application issues or implement software updates.

External Communications

During the disaster recovery process, it will be necessary to communicate with various entities outside your organization. You will need to contact vendors to provide supplies as they are needed to support the disaster recovery effort. Your clients will want to contact you for reassurance that you are still in operation. Public relations officials may need to contact the media or investment firms, and managers may need to speak to governmental authorities. For these reasons, it is essential that your disaster recovery plan include appropriate channels of communication to the outside world in a quantity sufficient to meet your operational needs. Usually, it is not a sound business practice or recovery practice to use the CEO as your spokesperson during a disaster. A media liaison should be hired, trained, and prepared to take on this responsibility.

Utilities

As discussed in previous sections of this chapter, your organization is reliant upon several utilities to provide critical elements of your infrastructure—electric power, water, natural gas, sewer service, and so on. Your disaster recovery plan should contain contact information and procedures to troubleshoot these services if problems arise during a disaster.

Logistics and Supplies

The logistical problems surrounding a disaster recovery operation are immense. You will suddenly face the problem of moving large numbers of people, equipment, and supplies to alternate recovery sites. It’s also possible that the people will be actually living at those sites for an extended period of time and that the disaster recovery team will be responsible for providing them with food, water, shelter, and appropriate facilities. Your disaster recovery plan should contain provisions for this type of operation if it falls within the scope of your expected operational needs.

Recovery vs. Restoration

It is sometimes useful to separate disaster recovery tasks from disaster restoration tasks. This is especially true when a recovery effort is expected to take a significant amount of time. A disaster recovery team may be assigned to implement and maintain operations at the recovery site, while a salvage team is assigned to restore the primary site to operational capacity. Make these allocations according to the needs of your organization and the types of disasters you face.

NOTE

> *Recovery* and *restoration* are separate concepts. In this context, recovery involves restoring business operations and processes to a working state. Restoration involves restoring a business facility and environment to a workable state.

The recovery team members have a very short time frame in which to operate. They must put the DRP into action and restore IT capabilities as swiftly as possible. If the recovery team fails to restore business processes within the MTD/RTO, then the company fails.

Once the original site is deemed safe for people, the salvage team members begin their work. Their job is to restore the company to its full original capabilities and, if necessary, to the original location. If the original location is no longer in existence, then a new primary spot is selected. The salvage team must rebuild or repair the IT infrastructure. Since this activity is basically the same as building a new IT system, the return activity from the alternate/recovery site to the primary/original site is itself a risky activity. Fortunately, the salvage team has more time to work than the recovery team.

The salvage team must ensure the reliability of the new IT infrastructure. This is done by returning the least-mission-critical processes to the restored original site to stress-test the rebuilt network. As the restored site shows resiliency, more important processes are transferred. A serious vulnerability exists when mission-critical processes are returned to the original site. The act of returning to the original site could cause a disaster of its own. Therefore, the state of emergency cannot be declared over until full normal operations have returned to the restored original site.

At the conclusion of any disaster recovery effort, the time will come to restore operations at the primary site and terminate any processing sites operating under the disaster recovery agreement. Your DRP should specify the criteria used to determine when it is appropriate to return to the primary site and guide the DRP recovery and salvage teams through an orderly transition.

Training and Documentation

As with a business continuity plan, it is essential that you provide training to all personnel who will be involved in the disaster recovery effort. The level of training required will vary according to an individual's role in the effort and their position within the company. When designing a training plan, consider including the following elements:

- Orientation training for all new employees
- Initial training for employees taking on a new disaster recovery role for the first time
- Detailed refresher training for disaster recovery team members
- Brief refresher training for all other employees (can be accomplished as part of other meetings and through a medium like email newsletters sent to all employees)

TIP

> Loose-leaf binders are an excellent way to store disaster recovery plans. You can distribute single-page changes to the plan without destroying a national forest!

The disaster recovery plan should also be fully documented. Earlier in this chapter, we discussed several of the documentation options available to you. Be sure you implement the necessary documentation programs and modify the documentation as changes to the plan occur. Because of the rapidly changing nature of the disaster recovery and business continuity plans, you might consider publication on a secured portion of your organization's intranet.

Your DRP should be treated as an extremely sensitive document and provided to individuals on a compartmentalized, need-to-know basis only. Individuals who participate in the plan should understand their roles fully, but they do not need to know or have access to the entire plan. Of course, it is essential to ensure that key DRP team members and senior management have access to the entire plan and understand the high-level implementation details. You certainly don't want this knowledge to rest in the mind of one individual.

WARNING

> Remember that a disaster may render your intranet unavailable. If you choose to distribute your disaster recovery and business continuity plans

through an intranet, be sure you maintain an adequate number of printed copies of the plan at both the primary and alternate sites and maintain *only* the most current copy!

Testing and Maintenance

Every disaster recovery plan must be tested on a periodic basis to ensure that the plan's provisions are viable and that it meets an organization's changing needs. The types of tests that you conduct will depend on the types of recovery facilities available to you, the culture of your organization, and the availability of disaster recovery team members. The five main test types—checklist tests, structured walk-throughs, simulation tests, parallel tests, and full-interruption tests—are discussed in the remaining sections of this chapter.

Checklist Test

The *checklist test* is one of the simplest tests to conduct, but it's also one of the most critical. In this test, you simply distribute copies of disaster recovery checklists to the members of the disaster recovery team for review. This lets you accomplish three goals simultaneously:

- It ensures that key personnel are aware of their responsibilities and have that knowledge refreshed periodically.
- It provides individuals with an opportunity to review the checklists for obsolete information and update any items that require modification because of changes within the organization.
- In large organizations, it helps identify situations in which key personnel have left the company and nobody bothered to reassign their disaster recovery responsibilities. This is also a good reason why disaster recovery responsibilities should be included in job descriptions.

Structured Walk-Through

A *structured walk-through* takes testing one step further. In this type of test, often referred to as a *table-top exercise*, members of the disaster recovery team gather in a large conference room and role-play a disaster scenario. Usually, the exact scenario is known only to the test moderator, who presents the details to the team at the meeting. The team members then refer to their copies of the disaster recovery plan and discuss the appropriate responses to that particular type of disaster.

Simulation Test

Simulation tests are similar to the structured walk-throughs. In simulation tests, disaster recovery team members are presented with a scenario and asked to develop an appropriate response. Unlike with the tests previously discussed, some of these response measures are then tested. This may involve the interruption of noncritical business activities and the use of some operational personnel.

Parallel Test

Parallel tests represent the next level in testing and involve relocating personnel to the alternate recovery site and implementing site activation procedures. The employees relocated to the site perform their disaster recovery responsibilities just as they would for an actual disaster. The only difference is that operations at the main facility are not interrupted. That site retains full responsibility for conducting the day-to-day business of the organization.

Full-Interruption Test

Full-interruption tests operate like parallel tests, but they involve actually shutting down operations at the primary site and shifting them to the recovery site. For obvious reasons, full-interruption tests are extremely difficult to arrange, and you often encounter resistance from management.

Maintenance

Remember that a disaster recovery plan is a living document. As your organization’s needs change, you must adapt the disaster recovery plan to meet those changed needs to follow suit. You will discover many necessary modifications by using a well-organized and coordinated testing plan. Minor changes may often be made through a series of telephone conversations or emails, whereas major changes may require one or more meetings of the full disaster recovery team.

A disaster recovery planner should refer to the organization’s business continuity plan as a template for its recovery efforts. This and all the supportive material must comply with federal regulations and reflect current business needs. Business processes such as payroll and order generation should contain specified metrics mapped to related IT systems and infrastructure.

Most organizations apply formal change management processes so that whenever the IT infrastructure changes, all relevant documentation is updated and checked to reflect such changes. Regularly scheduled fire drills and dry runs to ensure that all elements of the DRP are used properly to keep staff trained present a perfect opportunity to integrate changes into regular maintenance and change management procedures. Design, implement, and document changes each time you go through these processes and exercises. Know where everything is, and keep each element of the DRP working properly. In case of emergency, use your recovery plan. Finally, make sure the staff stays trained to keep their skills sharp—for existing support personnel—and use simulated exercises to bring new people up to speed quickly.

Summary

Disaster recovery planning is critical to a comprehensive information security program. No matter how comprehensive your business continuity plan, the day may come when your business is interrupted by a disaster and you face the task of restoring operations to the primary site quickly and efficiently. Recall the old adage that “an ounce of prevention is worth a pound of cure.” Spending the time and effort to develop a comprehensive disaster recovery plan greatly aids the process of recovering operations amidst a chaotic emergency.

An organization’s disaster recovery plan is one of the most important documents under the purview of security professionals. It should provide guidance to the personnel responsible for ensuring the continuity of operations in the face of disaster. The DRP provides an orderly sequence of events designed to activate alternate processing sites while simultaneously restoring the primary site to operational status. Security professionals should ensure that adequate programs are in place so that those team members charged with disaster recovery duties are well trained for their roles under the plan.

Exam Essentials

Know the common types of natural disasters that may threaten an organization. Natural disasters that commonly threaten organizations include earthquakes, floods, storms, fires, tsunamis, and volcanic eruptions.

Know the common types of man-made disasters that may threaten an organization. Explosions, electrical fires, terrorist acts, power outages, other utility failures, infrastructure failures, hardware/software failures, labor difficulties, theft, and vandalism are all common man-made disasters.

Be familiar with the common types of recovery facilities. The common types of recovery facilities are cold sites, warm sites, hot sites, mobile sites, service bureaus, and multiple sites. Be sure you understand the benefits and drawbacks for each such facility.

Explain the potential benefits behind mutual assistance agreements as well as the reasons they are not commonly implemented in businesses today. Mutual assistance agreements (MAAs) provide an inexpensive alternative to disaster recovery sites, but they are not commonly used because they are difficult to enforce. Organizations participating in an MAA may also be shut down by the same disaster, and MAAs raise confidentiality concerns.

Know the five types of disaster recovery plan tests and the impact each has on normal business operations. The five types of disaster recovery plan tests are checklist tests, structured walk-throughs, simulation tests, parallel tests, and full-interruption tests. Checklist tests are purely paperwork exercises, whereas structured walk-throughs involve a project team meeting. Neither has an impact on business operations. Simulation tests may shut down noncritical business units. Parallel tests involve relocating personnel but do not affect day-to-day operations. Full-interruption tests involve shutting down primary systems and shifting responsibility to the recovery facility.

Written Lab

1. What are some of the main concerns businesses have when considering adopting a mutual assistance agreement?

2. List and explain the five types of disaster recovery tests.

3. Explain the differences between the three types of backup strategies discussed in this chapter.

Answers to Written Lab

1. Businesses have three main concerns when considering adopting a mutual assistance agreement. First, the nature of an MAA often necessitates that the businesses be located in close geographical proximity. However, this requirement also increases the risk that the two businesses will fall victim to the same threat. Second, MAAs are difficult to enforce in the middle of a crisis. If one of the organizations is affected by a disaster and the other isn't, the organization not affected could back out at the last minute, and the other organization is out of luck. Finally, confidentiality concerns (both legal and business related) often prevent businesses from trusting others with their sensitive operational data.

2. There are five main types of disaster recovery tests:

- Checklist tests involve the distribution of recovery checklists to disaster recovery personnel for review.
- Structured walk-throughs are "table-top" exercises that involve assembling the disaster recovery team to discuss a disaster scenario.
- Simulation tests are more comprehensive and may impact one or more noncritical business units of the organization.
- Parallel tests involve relocating personnel to the alternate site and commencing operations there.
- Full-interruption tests involve relocating personnel to the alternate site and shutting down operations at the primary site.

3. Full backups create a copy of all data stored on a server. Incremental backups create copies of all files modified since the last full or incremental backup. Differential backups create copies of all files modified since the last full backup without regard to any previous differential or incremental backups that may have taken place.

Review Questions

1. What is the end goal of disaster recovery planning?

A. Preventing business interruption

B. Setting up temporary business operations

C. Restoring normal business activity

D. Minimizing the impact of a disaster

2. Which one of the following is an example of a man-made disaster?

A. Tsunami

B. Earthquake

C. Power outage

D. Lightning strike

3. According to the Federal Emergency Management Agency, approximately what percentage of U.S. states is rated with at least a moderate risk of seismic activity?

A. 20 percent

B. 40 percent

C. 60 percent

D. 80 percent

4. Which one of the following disaster types is not usually covered by standard business or homeowner’s insurance?

A. Earthquake

B. Flood

C. Fire

D. Theft

5. In the wake of the September 11, 2001, terrorist attacks, what industry made drastic changes that directly impact DRP/BCP activities?

A. Tourism

B. Banking

C. Insurance

D. Airline

6. Which of the following statements about business continuity planning and disaster recovery planning is incorrect?

A. Business continuity planning is focused on keeping business functions uninterrupted when a disaster strikes.

B. Organizations can choose whether to develop business continuity planning or disaster recovery planning plans.

C. Business continuity planning picks up where disaster recovery planning leaves off.

D. Disaster recovery planning guides an organization through recovery of normal operations at the primary facility.

7. What does the term "100-year flood plain" mean to emergency preparedness officials?

A. The last flood of any kind to hit the area was more than 100 years ago.

B. The odds of a flood at this level are 1 in 100 in any given year.

C. The area is expected to be safe from flooding for at least 100 years.

D. The last significant flood to hit the area was more than 100 years ago.

8. In which one of the following database recovery techniques is an exact, up-to-date copy of the database maintained at an alternative location?

A. Transaction logging

B. Remote journaling

C. Electronic vaulting

D. Remote mirroring

9. What disaster recovery principle best protects your organization against hardware failure?

A. Consistency

B. Efficiency

C. Redundancy

D. Primacy

10. What business continuity planning technique can help you prepare the business unit prioritization task of disaster recovery planning?

A. Vulnerability analysis

B. Business impact analysis

C. Risk management

D. Continuity planning

11. Which one of the following alternative processing sites takes the longest time to activate?

A. Hot site

B. Mobile site

C. Cold site

D. Warm site

12. What is the typical time estimate to activate a warm site from the time a disaster is declared?

A. 1 hour

B. 6 hours

C. 12 hours

D. 24 hours

13. Which one of the following items is a characteristic of hot sites but not a characteristic of warm sites?

A. Communications circuits

B. Workstations

C. Servers

D. Current data

14. What type of database backup strategy involves maintenance of a live backup server at the remote site?

A. Transaction logging

B. Remote journaling

C. Electronic vaulting

D. Remote mirroring

15. What type of document will help public relations specialists and other individuals who need a high-level summary of disaster recovery efforts while they are underway?

A. Executive summary

B. Technical guides

C. Department-specific plans

D. Checklists

16. What disaster recovery planning tool can be used to protect an organization against the failure of a critical software firm to provide appropriate support for their products?

A. Differential backups

B. Business impact assessment

C. Incremental backups

D. Software escrow agreement

17. What type of backup involves always storing copies of all files modified since the most recent full backup?

A. Differential backups

B. Partial backup

C. Incremental backups

D. Database backup

18. What combination of backup strategies provides the fastest backup creation time?

A. Full backups and differential backups

B. Partial backups and incremental backups

C. Full backups and incremental backups

D. Incremental backups and differential backups

19. What combination of backup strategies provides the fastest backup restoration time?

A. Full backups and differential backups

B. Partial backups and incremental backups

C. Full backups and incremental backups

D. Incremental backups and differential backups

20. What type of disaster recovery plan test fully evaluates operations at the backup facility but does not shift primary operations responsibility from the main site?

A. Structured walk-through

B. Parallel test

C. Full-interruption test

D. Simulation test

Answers to Review Questions

1. C. Once a disaster interrupts the business operations, the goal of DRP is to restore regular business activity as quickly as possible. Thus, disaster recovery planning picks up where business continuity planning leaves off.

2. C. A power outage is an example of a man-made disaster. The other events listed—tsunamis, earthquakes, and lightning strikes—are all naturally occurring events.

3. D. As shown in Table 16.1, 41 of the 50 U.S. states are considered to have a moderate, high, or very high risk of seismic activity. This rounds to 80 percent to provide the value given in answer D.

4. B. Most general business insurance and homeowner's insurance policies do not provide any protection against the risk of flooding or flash floods. If floods pose a risk to your organization, you should consider purchasing supplemental flood insurance under FEMA's National Flood Insurance Program.

5. C. Although all the industries listed in the options made changes to their practices after September 11, 2001, the insurance industry's change toward noncoverage of acts of terrorism most directly impacts the BCP/DRP process.

6. C. The opposite of this statement is true—disaster recovery planning picks up where business continuity planning leaves off. The other three statements are all accurate reflections of the role of business continuity planning and disaster recovery planning.

7. B. The term *100-year flood plain* is used to describe an area where flooding is expected once every 100 years. It is, however, more mathematically correct to say that this labels indicates a 1 percent probability of flooding in any given year.

8. D. When you use remote mirroring, an exact copy of the database is maintained at an alternative location. You keep the remote copy up-to-date by executing all transactions on both the primary and remote site at the same time.

9. C. Redundant systems/components provide protection against the failure of one particular piece of hardware.

10. B. During the business impact assessment phase, you must identify the business priorities of your organization to assist with the allocation of BCP resources. You can use this same information to drive the DRP business unit prioritization.

11. C. The cold site contains none of the equipment necessary to restore operations. All of the equipment must be brought in and configured and data must be restored to it before operations can commence. This often takes weeks.

12. C. Warm sites typically take about 12 hours to activate from the time a disaster is declared. This is compared to the relatively instantaneous activation of a hot site and the lengthy (at least a week) time required to bring a cold site to operational status.

13. D. Warm sites and hot sites both contain workstations, servers, and the communications circuits necessary to achieve operational status. The main difference between the two alternatives is the fact that hot sites contain near real-time copies of the operational data and warm sites require the restoration of data from backup.

14. D. Remote mirroring is the only backup option in which a live backup server at a remote site maintains a bit-for-bit copy of the contents of the primary server, synchronized as closely as the latency in the link between primary and remote systems will allow.

15. A. The executive summary provides a high-level view of the entire organization’s disaster recovery efforts. This document is useful for the managers and leaders of the firm as well as public relations personnel who need a nontechnical perspective on this complex effort.

16. D. Software escrow agreements place the application source code in the hands of an independent third party, thus providing firms with a “safety net” in the event a developer goes out of business or fails to honor the terms of a service agreement.

17. A. Differential backups involve always storing copies of all files modified since the most recent full backup regardless of any incremental or differential backups created during the intervening time period.

18. C. Any backup strategy must include full backups at some point in the process. Incremental backups are created faster than differential backups because of the number of files it is necessary to back up each time.

19. A. Any backup strategy must include full backups at some point in the process. If a combination of full and differential backups is used, a maximum of two backups must be restored. If a combination of full and incremental backups is chosen, the number of required restorations may be unlimited.

20. B. Parallel tests involve moving personnel to the recovery site and gearing up operations, but responsibility for conducting day-to-day operations of the business remains at the primary operations center.

Chapter 17

Law and Investigations

THE CISSP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

- **Legal, Regulations, Investigations, and Compliance**
    - Understand legal issues that pertain to information security internationally
        - Computer crime; licensing and intellectual property (e.g., copyright, trademark); import/export; trans-border data flow; privacy
    - Understand and support investigations
        - Policy; incident handling and response; evidence collection and handling (e.g., chain of custody, interviewing); reporting and documenting
    - Understand forensic procedures
        - Media analysis; network analysis; software analysis
    - Understand compliance requirements and procedures
        - Regulatory environment; audits; reporting
- **Operations Security**
    - Manage incident response
        - Detection; response; reporting; recovery; remediation

In the early days of computer security, information security professionals were pretty much left on their own to defend their systems against attacks. They didn't have much help from the criminal and civil justice systems. When they did seek assistance from law enforcement, they were met with reluctance by overworked agents who didn't have a basic understanding of how something that involved a computer could actually be a crime. The legislative branch of government hadn't addressed the issue of computer crime, and the executive branch thought they simply didn't have statutory authority or obligation to pursue those matters.

Fortunately, both our legal system and the men and women of law enforcement have come a long way over the past two decades. The legislative branches of governments around the world have at least attempted to address issues of computer crime. Many law enforcement agencies have full-time, well-trained computer crime investigators with advanced security training. Those that don't usually know where to turn when they require this sort of experience.

In this chapter, we'll cover the various types of laws that deal with computer security issues. We'll examine the legal issues surrounding computer crime, privacy, intellectual property, and a number of other related topics. We'll also cover basic investigative techniques, including the pros and cons of calling in assistance from law enforcement.

Categories of Laws

Three main categories of laws play a role in our legal system. Each is used to cover a variety of different circumstances, and the penalties for violating laws in the different categories vary widely. In the following sections, we'll cover how criminal law, civil law, and administrative law interact to form the complex web of our justice system.

Criminal Law

Criminal law forms the bedrock of the body of laws that preserve the peace and keep our society safe. Many high-profile court cases involve matters of criminal law; these are the laws that the police and other law enforcement agencies concern themselves with. Criminal law contains prohibitions against acts such as murder, assault, robbery, and arson. Penalties for violating criminal statutes fall in a range that includes mandatory hours of community service, monetary penalties in the form of fines (small and large), and deprivation of civil liberties in the form of prison sentences.

Cops Are Smart!

A good friend of one of the authors is a technology crime investigator for the local police department. He often receives cases of computer abuse involving threatening emails and website postings.

Recently, he shared a story about a bomb threat that had been emailed to a local high school. The perpetrator sent a threatening note to the school principal declaring that the bomb would explode at 1 p.m. and warning him to evacuate the school. The author's friend received the alert at 11 a.m., leaving him with only two hours to investigate the crime and advise the principal on the best course of action.

He quickly began issuing emergency subpoenas to Internet service providers and traced the email to a computer in the school library. At 12:15 p.m., he confronted the suspect with surveillance tapes showing him at the computer in the library as well as audit logs conclusively proving that he had sent the email. The student quickly admitted that the threat was nothing more than a ploy to get out of school a couple of hours early. His explanation? "I didn't think there was anyone around here who could trace stuff like that."

He was wrong.

A number of criminal laws serve to protect society against computer crime. In later sections of this chapter, you'll learn how some laws, such as the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the Identity Theft and Assumption Deterrence Act (among others), provide criminal penalties for serious cases of computer crime. Technically savvy prosecutors teamed with concerned law enforcement agencies have dealt serious blows to the "hacking underground" by using the court system to slap lengthy prison terms on offenders guilty of what used to be considered harmless pranks.

In the United States, legislative bodies at all levels of government establish criminal laws through elected representatives. At the federal level, both the House of Representatives and the Senate must pass criminal law bills by a majority vote (in most cases) in order for the bill to become law.

Once passed, these laws then become federal law and apply in all cases where the federal government has jurisdiction (mainly cases that involve interstate commerce, cases that cross state boundaries, or cases that are offenses against the federal government itself). If federal jurisdiction does not apply, state authorities handle the case using laws passed in a similar manner by state legislators.

All federal and state laws must comply with the document that dictates how the U.S. system of government works—the U.S. Constitution. All laws are subject to judicial review by regional courts with the right of appeal all the way to the Supreme Court of the United States. If a court finds that a law is unconstitutional, it has the power to strike it down and render it invalid.

Keep in mind that criminal law is a serious matter. If you find yourself involved—either as a witness, defendant, or victim—in a matter where criminal authorities become involved, you'd be well advised to seek advice from an attorney familiar with the criminal justice system and specifically with matters of computer crime. It's not wise to "go it alone" in such a complex system.

Civil Law

Civil laws form the bulk of our body of laws. They are designed to provide for an orderly society and govern matters that are not crimes but require an impartial arbiter to settle between individuals and organizations. Examples of the types of matters that may be judged under civil law include contract disputes, real estate transactions, employment matters, and estate/probate procedures. Civil laws also are used to create the framework of government that the executive branch uses to carry out its responsibilities. These laws provide budgets for governmental activities and lay out the authority granted to the executive branch to create administrative laws (see the next section).

Civil laws are enacted in the same manner as criminal laws. They must pass through the legislative process before enactment and are subject to the same constitutional parameters and judicial review procedures. At the federal level, both criminal and civil laws are embodied in the United States Code (USC).

The major difference between civil laws and criminal laws is the way in which they are enforced. Usually, law enforcement authorities do not become involved in matters of civil law beyond taking action necessary to restore order. In a criminal prosecution, the government, through law enforcement investigators and prosecutors, brings action against a person accused of a crime. In civil matters, it is incumbent upon the person who thinks they have been wronged to obtain legal counsel and file a civil lawsuit against the person they think is responsible for their grievance. The government (unless it is the plaintiff or defendant) does not take sides in the dispute or argue one position or the other. The only role of the government in civil matters is to provide the judges, juries, and court facilities used to hear civil cases and to play an administrative role in managing the judicial system in accordance with the law.

As with criminal law, it is best to obtain legal assistance if you think you need to file a civil lawsuit or someone files a civil lawsuit against you. Although civil law does not impose the threat of imprisonment, the losing party may face severe financial penalties. You don't need to look any further than the nightly news for examples—multimillion-dollar cases against tobacco companies, major corporations, and wealthy individuals are filed every day.

Administrative Law

The executive branch of our government charges numerous agencies with wide-ranging responsibilities to ensure that government functions effectively. It is the duty of these agencies to abide by and enforce the criminal and civil laws enacted by the legislative branch. However, as can be easily imagined, criminal and civil law can't possibly lay out rules and procedures that should be followed in any possible situation. Therefore, executive branch agencies have some leeway to enact administrative law, in the form of policies, procedures, and regulations that govern the daily operations of the agency. Administrative law covers topics as mundane as the procedures to be used within a federal agency to obtain a desk telephone to more substantial issues such as the immigration policies that will be used to enforce the laws passed by Congress. Administrative law is published in the Code of Federal Regulations, often referred to as the CFR.

Although administrative law does not require an act of the legislative branch to gain the force of law, it must comply with all existing civil and criminal laws. Government agencies may not implement regulations that directly contradict existing laws passed by the legislature. Furthermore, administrative laws (and the actions of government agencies) must also comply with the U.S. Constitution and are subject to judicial review.

In order to understand compliance requirements and procedures, it is necessary to be fully versed in the complexities of the law. From administrative law to civil law to criminal law (and, in some countries, even religious law), navigating the regulatory environment is a daunting task. The CISSP exam focuses on the generalities of law, regulations, investigations, and compliance. However, it is your responsibility to seek out professional help (i.e., an attorney) to guide and support you in your efforts to maintain legal and legally supportable security.

Laws

Throughout these sections, we'll examine a number of laws that relate to information technology. By necessity, this discussion is U.S.-centric, as is the material covered by the CISSP exam. We'll look at several high-profile foreign laws, such as the European Union's data privacy act. However, if you operate in an environment that involves foreign jurisdictions, you should retain local legal counsel to guide you through the system.

WARNING

> Every information security professional should have a basic understanding of the law as it relates to information technology. However, the most important lesson to be learned is knowing when it's necessary to call in an attorney: If you think you're in a legal "gray area," it's best to seek professional advice.

Computer Crime

The first computer security issues addressed by legislators were those involving computer crime. Early computer crime prosecutions were attempted under traditional criminal law, and many were dismissed because judges thought that applying traditional law to this modern type of crime was too far of a stretch. Legislators responded by passing specific statutes that defined computer crime and laid out specific penalties for various crimes. In the following sections, we'll cover several of those statutes.

> The U.S. laws discussed in this chapter are federal laws. Almost every state in the union has enacted some form of legislation regarding computer security issues. Because of the global reach of the Internet, most computer crimes cross state lines and, therefore, fall under federal jurisdiction and are prosecuted in the federal court system. However, in some circumstances, state laws can be more restrictive than federal laws and impose harsher penalties.

Computer Fraud and Abuse Act of 1984

Congress first enacted the Computer Fraud and Abuse Act (CFAA) in 1984, and it remains in force today, with several amendments. This law was carefully written to exclusively cover computer crimes that crossed state boundaries to avoid infringing upon states' rights and treading on thin constitutional ice. The major provisions of the act are that it is a crime to perform the following:

- Access classified information or financial information in a federal system without authorization or in excess of authorized privileges.
- Access a computer used exclusively by the federal government without authorization.
- Use a federal computer to perpetrate a fraud (unless the only object of the fraud was to gain use of the computer itself).
- Cause malicious damage to a federal computer system in excess of $1,000.
- Modify medical records in a computer when doing so impairs or may impair the examination, diagnosis, treatment, or medical care of an individual.
- Traffic in computer passwords if the trafficking affects interstate commerce or involves a federal computer system.

The CFAA was amended in 1986 to change the scope of the act. Instead of merely covering federal computers that processed sensitive information, the act was changed to cover all "federal interest" computers. This widened the coverage of the act to include the following:

- Any computer used exclusively by the U.S. government
- Any computer used exclusively by a financial institution
- Any computer used by the government or a financial institution when the offense impedes the ability of the government or institution to use that system
- Any combination of computers used to commit an offense when they are not all located in the same state

> When preparing for the CISSP exam, be sure you’re able to briefly describe the purpose of each law discussed in this chapter.

1994 CFAA Amendments

In 1994, Congress recognized that the face of computer security had drastically changed since the CFAA was last amended in 1986 and made a number of sweeping changes to the act. Collectively, these changes are referred to as the Computer Abuse Amendments Act of 1994 and included the following provisions:

- Outlawed the creation of any type of malicious code that might cause damage to a computer system
- Modified the CFAA to cover any computer used in interstate commerce rather than just “federal interest” computer systems
- Allowed for the imprisonment of offenders, regardless of whether they actually intended to cause damage
- Provided legal authority for the victims of computer crime to pursue civil action to gain injunctive relief and compensation for damages

Computer Security Act of 1987

After amending the CFAA in 1986 to cover a wider variety of computer systems, Congress turned its view inward and examined the current state of computer security in federal government systems. Members of Congress were not satisfied with what they saw and enacted the Computer Security Act (CSA) of 1987 to mandate baseline security requirements for all federal agencies. In the introduction to the CSA, Congress specified four main purposes of the act:

- To give the National Institute of Standards and Technology (NIST) responsibility for developing standards and guidelines for federal computer systems. For this purpose, NIST draws on the technical advice and assistance (including work products) of the National Security Agency where appropriate.

- To provide for the enactment of such standards and guidelines.
- To require the establishment of security plans by all operators of federal computer systems that contain sensitive information.
- To require mandatory periodic training for all people involved in management, use, or operation of federal computer systems that contain sensitive information.

This act clearly set out a number of requirements that formed the basis of federal computer security policy for many years. It also divided responsibility for computer security among two federal agencies. The National Security Agency (NSA), which formerly had authority over all computer security issues, now retained authority over classified systems. NIST gained responsibility for securing all other federal government systems and produces the 800 series of Special Publications related to computer security in the federal government. These are useful for all security practitioners and are available for free online at http://csrc.nist.gov/publications/PubsSPs.html.

Federal Sentencing Guidelines

The Federal Sentencing Guidelines released in 1991 provided punishment guidelines to help federal judges interpret computer crime laws. Three major provisions of these guidelines have had a lasting impact on the information security community:

- The guidelines formalized the *prudent man rule*, which requires senior executives to take personal responsibility for ensuring the *due care* that ordinary, prudent individuals would exercise in the same situation. This rule, developed in the realm of fiscal responsibility, now applies to information security as well.
- The guidelines allowed organizations and executives to minimize punishment for infractions by demonstrating that they used due diligence in the conduct of their information security duties.
- The guidelines outlined three burdens of proof for *negligence*. First, there must be a legally recognized obligation of the person accused of negligence. Second, the person must have failed to comply with recognized standards. Finally, there must be a causal relationship between the act of negligence and subsequent damages.

Paperwork Reduction Act of 1995

The Paperwork Reduction Act of 1995 requires that agencies obtain Office of Management and Budget (OMB) approval before requesting most types of information from the public. Information collections include forms, interviews, record-keeping requirements, and a wide variety of other things. The Government Information Security Reform Act (GISRA) of 2000 amended this act.

National Information Infrastructure Protection Act of 1996

In 1996, Congress passed yet another set of amendments to the Computer Fraud and Abuse Act designed to further extend the protection it provides. The National Information Infrastructure Protection Act included the following main new areas of coverage:

- Broadens CFAA to cover computer systems used in international commerce in addition to systems used in interstate commerce
- Extends similar protections to portions of the national infrastructure other than computing systems, such as railroads, gas pipelines, electric power grids, and telecommunications circuits
- Treats any intentional or reckless act that causes damage to critical portions of the national infrastructure as a felony

Government Information Security Reform Act of 2000

The Government Information Security Reform Act (GISRA) of 2000 amends the United States Code to implement additional information security policies and procedures. In the text of the act, Congress laid out five basic purposes for establishing the GISRA:

- To provide a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support federal operations and assets
- To recognize the highly networked nature of the federal computing environment, including the need for federal government interoperability, and in the implementation of improved security management measures, to assure that opportunities for interoperability are not adversely affected
- To provide effective government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities
- To provide for development and maintenance of minimum controls required to protect federal information and information systems
- To provide a mechanism for improved oversight of federal agency information security programs

The provisions of the GISRA continue to charge the National Institute of Standards and Technology and the National Security Agency with security oversight responsibilities for unclassified and classified information processing systems, respectively. However, GISRA places the burden of maintaining the security and integrity of government information and information systems squarely on the shoulders of individual agency leaders.

GISRA also creates a new category of computer system. A mission-critical system meets one of the following criteria:

- It is defined as a national security system by other provisions of law.
- It is protected by procedures established for classified information.
- The loss, misuse, disclosure, or unauthorized access to or modification of any information it processes would have a debilitating impact on the mission of an agency.

GISRA provides specific evaluation and auditing authority for mission-critical systems to the secretary of defense and the director of central intelligence. This is an attempt to ensure that all government agencies, even those that do not routinely deal with classified national security information, implement adequate security controls on systems that are absolutely critical to the continued functioning of the agency.

Intellectual Property

America’s role in the global economy is shifting away from a manufacturer of goods and toward a provider of services. This trend also shows itself in many of the world’s large industrialized nations. With this shift toward providing services, intellectual property takes on an increasingly important role in many firms. Indeed, it is arguable that the most valuable assets of many large multinational companies are simply the brand names that we’ve all come to recognize, and company names such as Dell, Procter & Gamble, and Merck bring instant credibility to any product. Publishing companies, movie producers, and artists depend upon their creative output to earn their livelihood. Many products depend upon secret recipes or production techniques—take the legendary secret formula for Coca-Cola or the Colonel’s secret blend of herbs and spices, for example.

These intangible assets are collectively referred to as *intellectual property*, and a whole host of laws exist to protect the rights of their owners. After all, it simply wouldn’t be fair if a music store bought only one copy of each artist's CD and burned copies for all of its customers—that would deprive the artist of the benefits of their labor. In the following sections, we'll explore the laws surrounding the four major types of intellectual property—copyrights, trademarks, patents, and trade secrets. We'll also discuss how these concepts specifically concern information security professionals. Many countries protect (or fail to protect) these rights in different ways, but the basic concepts ring true throughout the world.

WARNING

> Some countries are notorious for violating intellectual property rights. The most notable example is China. China is world renowned for its blatant disregard of copyright and patent law. If you're planning to do business in this region of the world, you should definitely consult with an attorney who specializes in this area.

Copyrights and the Digital Millennium Copyright Act

Copyright law guarantees the creators of "original works of authorship" protection against the unauthorized duplication of their work. Eight broad categories of works qualify for copyright protection:

- Literary works
- Musical works
- Dramatic works
- Pantomimes and choreographic works
- Pictorial, graphical, and sculptural works
- Motion pictures and other audiovisual works
- Sound recordings
- Architectural works

There is precedent for copyrighting computer software—it's done under the scope of literary works. However, it's important to note that copyright law protects only the expression inherent in computer software—that is, the actual source code. It does not protect the ideas or process behind the software. There has also been some question over whether copyrights can be extended to cover the "look and feel" of a software package's graphical user interface. Court decisions have gone in both directions on this matter;

if you will be involved in this type of issue, you should consult a qualified intellectual property attorney to determine the current state of legislation and case law.

There is a formal procedure to obtain a copyright that involves sending copies of the protected work along with an appropriate registration fee to the U.S. Copyright Office. For more information on this process, visit the office's website at www.copyright.gov. However, it is important to note that officially registering a copyright is not a prerequisite for copyright enforcement. Indeed, the law states that the creator of a work has an automatic copyright from the instant the work is created. If you can prove in court that you were the creator of a work (perhaps by publishing it), you will be protected under copyright law. Official registration merely provides the government's acknowledgment that they received your work on a specific date.

Copyright ownership always defaults to the creator of a work. The exceptions to this policy are works for hire. A work is considered "for hire" when it is made for an employer during the normal course of an employee's workday. For example, when an employee in a company's public relations department writes a press release, the press release is considered a work for hire. A work may also be considered a work for hire when it is made as part of a written contract declaring it as such.

Current copyright law provides for a very lengthy period of protection. Works by one or more authors are protected until 70 years after the death of the last surviving author. Works for hire and anonymous works are provided protection for the shorter of 95 years from the date of first publication or 120 years from the date of creation.

In 1998, Congress recognized the rapidly changing digital landscape that was stretching the reach of existing copyright law. To help meet this challenge, it enacted the hotly debated Digital Millennium Copyright Act. The DMCA also serves to bring U.S. copyright law into compliance with terms of two World Intellectual Property Organization (WIPO) treaties.

The first major provision of the DMCA is the prohibition of attempts to circumvent copyright protection mechanisms placed on a protected work by the copyright holder. This clause was designed to protect copy-prevention mechanisms placed on digital media such as CDs and DVDs.

The DMCA provides for penalties of up to $1,000,000 and 10 years in prison for repeat offenders. Nonprofit institutions such as libraries and schools are exempted from this provision.

The DMCA also limits the liability of Internet service providers when their circuits are used by criminals violating the copyright law. The DMCA recognizes that ISPs have a legal status similar to the "common carrier" status of telephone companies and does not hold them liable for the "transitory activities" of their users. To qualify for this exemption, the service provider's activities must meet the following requirements (quoted directly from the Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary, December 1998):

- The transmission must be initiated by a person other than the provider.
- The transmission, routing, provision of connections, or copying must be carried out by an automated technical process without selection of material by the service provider.
- The service provider must not determine the recipients of the material.
- Any intermediate copies must not ordinarily be accessible to anyone other than anticipated recipients, and must not be retained for longer than reasonably necessary.
- The material must be transmitted with no modification to its content.

The DMCA also exempts activities of service providers related to system caching, search engines, and the storage of information on a network by individual users. However, in those cases, the service provider must take prompt action to remove copyrighted materials upon notification of the infringement.

Congress also included provisions in the DMCA that allow the creation of backup copies of computer software and any maintenance, testing, or routine usage activities that require software duplication. These provisions apply only if the software is licensed for use on a particular computer, the usage is in compliance with the license agreement, and any such copies are immediately deleted when no longer required for a permitted activity.

Finally, the DMCA spells out the application of copyright law principles to the emerging field of *webcasting*, or broadcasting audio and/or video content to recipients over the Internet. This technology is often referred to as *streaming audio* or *streaming video*. The DMCA states that these uses are to be treated as "eligible nonsubscription transmissions." The law in this area is still under development, so if you plan to engage in this type of activity, you should contact an attorney to ensure that you are in compliance with current law.

Trademarks

Copyright laws are used to protect creative works; there is also protection for *trademarks*, which are words, slogans, and logos used to identify a company and its products or services. For example, a business might obtain a copyright on its sales brochure to ensure that competitors can't duplicate its sales materials. That same business might also seek to obtain trademark protection for its company name and the names of specific products and services that it offers to its clients.

The main objective of trademark protection is to avoid confusion in the marketplace while protecting the intellectual property rights of people and organizations. As with copyright protection, trademarks do not need to be officially registered to gain protection under the law. If you use a trademark in the course of your public activities, you are automatically protected under any relevant trademark law and can use the ™ symbol to show that you intend to protect words or slogans as trademarks. If you want official recognition of your trademark, you can register it with the United States Patent and Trademark Office (USPTO). This process generally requires an attorney to perform a due diligence comprehensive search for existing trademarks that might preclude your registration. The entire registration process can take more than a year from start to finish. Once you've received your registration certificate from the USPTO, you can denote your mark as a registered trademark with the ® symbol.

One major advantage of trademark registration is that you may register a trademark that you intend to use but are not necessarily already using. This type of application is called an *intent to use* application and conveys trademark protection as of the date of filing provided that you actually use the trademark in commerce within a certain time period. If you opt not to register your trademark with the PTO, your protection begins only when you first use the trademark.

The acceptance of a trademark application in the United States depends on two main requirements:

- The trademark must not be confusingly similar to another trademark—you should determine this during your attorney's due diligence search. There will be an open opposition period during which other companies may dispute your trademark application.
- The trademark should not be descriptive of the goods and services that you will offer. For example, "Mike's Software Company" would not be a good trademark candidate because it describes the product produced by the company. The USPTO may reject an application if it considers the trademark descriptive.

In the United States, trademarks are granted for an initial period of 10 years and can be renewed for unlimited successive 10-year periods.

Patents

Patents protect the intellectual property rights of inventors. They provide a period of 20 years during which the inventor is granted exclusive rights to use the invention (whether directly or via licensing agreements). At the end of the patent exclusivity period, the invention is in the public domain available for anyone to use.

Patents have three main requirements:

- The invention must be new. Inventions are patentable only if they are original ideas.
- The invention must be useful. It must actually work and accomplish some sort of task.
- The invention must not be obvious. You could not, for example, obtain a patent for your idea to use a drinking cup to collect rainwater. This is an obvious solution. You might, however, be able to patent a specially designed cup that optimizes the amount of rainwater collected while minimizing evaporation.

In the technology field, patents have long been used to protect hardware devices and manufacturing processes. There is plenty of precedent on the side of inventors in those areas. Recent patents have also been issued covering software programs and similar mechanisms, but the jury is still out on whether these patents will hold up to the scrutiny of the courts.

Trade Secrets

Many companies have intellectual property that is absolutely critical to their business and significant damage would result if it were disclosed to competitors and/or the public—in other words, *trade secrets*. We previously mentioned two examples of this type of information from popular culture—the secret formula for Coca-Cola and Kentucky Fried Chicken's "secret blend of herbs and spices." Other examples are plentiful—a manufacturing company may want to keep secret a certain manufacturing process that only a few key employees fully understand, or a statistical analysis company might want to safeguard an advanced model developed for in-house use.

Two of the previously discussed intellectual property tools—copyrights and patents—could be used to protect this type of information, but with two major disadvantages:

- Filing a copyright or patent application requires that you publicly disclose the details of your work or invention. This automatically removes the "secret" nature of your property and may harm your firm by removing the mystique surrounding a product or by allowing unscrupulous competitors to copy your property in violation of international intellectual property laws.
- Copyrights and patents both provide protection for a limited period of time. Once your legal protection expires, other firms are free to use your work at will (and they have all the details from the public disclosure you made during the application process!).

There actually is an official process regarding trade secrets—by their nature you don't register them with anyone; you keep them to yourself. To preserve trade secret status, you must implement adequate controls within your organization to ensure that only authorized personnel with a need to know the secrets have access to them. You must also ensure that anyone who does have this type of access is bound by a nondisclosure agreement (NDA) that prohibits them from sharing the information with others and provides penalties for violating the agreement. Consult an attorney to ensure that the agreement lasts for the maximum period permitted by law. In addition, you must take steps to demonstrate that you value and protect your intellectual property. Failure to do so may result in the loss of trade secret protection.

Trade secret protection is one of the best ways to protect computer software. As discussed in the previous section, patent law does not provide adequate protection for computer software products. Copyright law protects only the actual text of the source code and doesn't prohibit others from rewriting your code in a different form and accomplishing the same objective. If you treat your source code as a trade secret, it keeps it out of the hands of your competitors in the first place. This is the technique used by large software development companies such as Microsoft to protect its core base of intellectual property.

Economic Espionage Act of 1996

Trade secrets are very often the crown jewels of major corporations, and the U.S. government recognized the importance of protecting this type of intellectual property when Congress enacted the Economic Espionage Act of 1996. This law has two major provisions:

- Anyone found guilty of stealing trade secrets from a U.S. corporation with the intention of benefiting a foreign government or agent may be fined up to $500,000 and imprisoned for up to 15 years.
- Anyone found guilty of stealing trade secrets under other circumstances may be fined up to $250,000 and imprisoned for up to 10 years.

The terms of the Economic Espionage Act give true teeth to the intellectual property rights of trade secret owners. Enforcing this law requires that companies take adequate steps to ensure that their trade secrets are well protected and not accidentally placed into the public domain.

Licensing

Security professionals should also be familiar with the legal issues surrounding software licensing agreements. Three common types of license agreements are in use today:

- *Contractual license agreements* utilize a written contract between the software vendor and the customer, outlining the responsibilities of each. These agreements are commonly found for high-priced and/or highly specialized software packages.
- *Shrink-wrap license agreements* are written on the outside of the software packaging. They commonly include a clause stating that you acknowledge agreement to the terms of the contract simply by breaking the shrink-wrap seal on the package.
- *Click-wrap license agreements* are becoming more commonplace than shrink-wrap agreements. In this type of agreement, the contract terms are either written on the software box or included in the software documentation. During the installation process, you are required to click a button indicating that you have read the terms of the agreement and agree to abide by them. This adds an active consent to the process, ensuring that the individual is aware of the agreement’s existence prior to installation.

Uniform Computer Information Transactions Act

The Uniform Computer Information Transactions Act (UCITA) is a federal law designed for adoption by each of the 50 states to provide a common framework for the conduct of computer-related business transactions. UCITA contains provisions that address software licensing. The terms of the UCITA give legal backing to the previously questionable practices of shrink-wrap licensing and click-wrap licensing by giving them status as legally binding contracts. UCITA also requires that manufacturers provide software users with the option to reject the terms of the license agreement before completing the installation process and receive a full refund of the software’s purchase price.

NOTE

Industry groups provide guidance and enforcement activities regarding software licensing. You can get more information from their websites. One major group is the Business Software Alliance (BSA) at www.bsa.org.

Import/Export

The federal government recognizes that the very same computers and encryption technologies that drive the Internet and e-commerce can be extremely powerful tools in the hands of a military force. For this reason, during the Cold War, the government developed a complex set of regulations governing the export of sensitive hardware and software products to other nations. The regulations include the management of trans-border data flow of new technologies, intellectual property, and personally identifying information.

Until recently, it was very difficult to export high-powered computers outside the United States, except to a select handful of allied nations. The controls on exporting encryption software were even more severe, rendering it virtually impossible to export any encryption technology outside the country. Recent changes in federal policy have relaxed these restrictions and provided for more open commerce.

Computer Export Controls

Currently, U.S. firms can export high-performance computing systems to virtually any country without receiving prior approval from the government. There are exceptions to this rule for countries designated by the Department of Commerce as Tier 3 countries. This includes countries such as India, Pakistan, Afghanistan, and many countries in the Middle East. The export of any computer that is capable of operating in excess of 0.75 weighted teraflops (a trillion floating-point operations per second) must be preapproved by the Department of Commerce.

NOTE

You can find a list of countries and their corresponding computer export tiers on the Department of Commerce's website at www.bis.doc.gov/hpcs.

The export of high-performance computers to any country currently on the Tier 4 list is prohibited. These countries include Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.

Encryption Export Controls

The Department of Commerce's Bureau of Industry and Security sets forth regulations on the export of encryption products outside the United States. Under previous regulations, it was virtually impossible to export even relatively low-grade encryption technology outside the United States. This placed U.S. software manufacturers at a great competitive disadvantage to foreign firms that faced no similar regulations. After a lengthy lobbying campaign by the software industry, the president directed the Commerce Department to revise its regulations to foster the growth of the American security software industry.

Current regulations now designate the categories of retail and mass market security software. The rules now permit firms to submit these products for review by the Commerce Department, but the review will take no longer than 30 days. After successful completion of this review, companies may freely export these products.

Privacy

The right to privacy has for years been a hotly contested issue in the United States. The main source of this contention is that the Constitution's Bill of Rights does not explicitly provide for a right to privacy. However, this right has been upheld by numerous courts and is vigorously pursued by organizations such as the American Civil Liberties Union (ACLU).

Europeans have also long been concerned with their privacy. Indeed, countries such as Switzerland are world renowned for their ability to keep financial secrets. Later in this chapter, we'll examine how the new European Union data privacy laws impact companies and Internet users.

U.S. Privacy Law

Although there is no constitutional guarantee of privacy, a myriad of federal laws (many enacted in recent years) are designed to protect the private information the government maintains about citizens as well as key portions of the private sector such as financial, educational, and health-care institutions. In the following sections, we'll examine a number of these federal laws.

Fourth Amendment

The basis for privacy rights is in the Fourth Amendment to the U.S. Constitution. It reads as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The direct interpretation of this amendment prohibits government agents from searching private property without a warrant and probable cause. The courts have expanded their interpretation of the Fourth Amendment to include protections against wiretapping and other invasions of privacy.

Privacy Act of 1974

The Privacy Act of 1974 is perhaps the most significant piece of privacy legislation restricting the way the federal government may deal with private information about individual citizens. It severely limits the ability of federal government agencies to disclose private information to other persons or agencies without the prior written consent of the affected individual(s). It does provide for exceptions involving the census, law enforcement, the National Archives, health and safety, and court orders.

The Privacy Act mandates that agencies maintain only the records that are necessary for conducting their business and that they destroy those records when they are no longer needed for a legitimate function of government. It provides a formal procedure for individuals to gain access to records the government maintains about them and to request that incorrect records be amended.

Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act (ECPA) makes it a crime to invade the electronic privacy of an individual. This act updated the Federal Wiretap Act to apply to the illegal interception of electronic (in other words, computer) communications or to the intentional, unauthorized access of electronically stored data. It prohibits the interception or disclosure of electronic communication and defines those situations in which disclosure is legal. It protects against the monitoring of email and voicemail communications and prevents providers of those services from making unauthorized disclosures of their content.

One of the most notable provisions of the ECPA is that it makes it illegal to monitor cellular telephone conversations. In fact, such monitoring is punishable by a fine of up to $500 and a prison term of up to five years.

Communications Assistance for Law Enforcement Act (CALEA) of 1994

The Communications Assistance for Law Enforcement Act (CALEA) of 1994 amended the Electronic Communications Privacy Act of 1986. CALEA requires all communications carriers to make wiretaps possible for law enforcement with an appropriate court order, regardless of the technology in use.

Economic and Protection of Proprietary Information Act of 1996

The Economic and Protection of Proprietary Information Act of 1996 extends the definition of property to include proprietary economic information so that the theft of this information can be considered industrial or corporate espionage. This changed the legal definition of theft so that it was no longer restricted by physical constraints.

Health Insurance Portability and Accountability Act of 1996

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which made numerous changes to the laws governing health insurance and health maintenance organizations (HMOs). Among the provisions of HIPAA are privacy and security regulations requiring strict security measures for hospitals, physicians, insurance companies, and other organizations that process or store private medical information about individuals.

> The HIPAA privacy and security regulations are quite complex. You should be familiar with the broad intentions of the act, as described here. If you work in the health-care industry, you should consider devoting time to an in-depth study of this law's provisions.

HIPAA also clearly defines the rights of individuals who are the subject of medical records and requires organizations that maintain such records to disclose these rights in writing.

Children's Online Privacy Protection Act of 1998

In April 2000, provisions of the Children's Online Privacy Protection Act (COPPA) became the law of the land in the United States. COPPA makes a series of demands upon websites that cater to children or knowingly collect information from children:

- Websites must have a privacy notice that clearly states the types of information they collect and what it's used for, including whether any information is disclosed to third parties. The privacy notice must also include contact information for the operators of the site.

- Parents must be provided with the opportunity to review any information collected from their children and permanently delete it from the site's records.
- Parents must give verifiable consent to the collection of information about children younger than the age of 13 prior to any such collection. Exceptions in the law allow websites to collect minimal information solely for the purpose of obtaining such parental consent.

Gramm-Leach-Bliley Act of 1999

Until the Gramm-Leach-Bliley Act (GLBA) became law in 1999, there were strict governmental barriers between financial institutions. Banks, insurance companies, and credit providers were severely limited in the services they could provide and the information they could share with each other. GLBA somewhat relaxed the regulations concerning the services each organization could provide. When Congress passed this law, it realized that this increased latitude could have far-reaching privacy implications. Because of this concern, it included a number of limitations on the types of information that could be exchanged even among subsidiaries of the same corporation and required financial institutions to provide written privacy policies to all their customers by July 1, 2001.

USA PATRIOT Act of 2001

Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 in direct response to the September 11, 2001, terrorist attacks in New York City and Washington, D.C. The PATRIOT Act greatly broadened the powers of law enforcement organizations and intelligence agencies across a number of areas, including when monitoring electronic communications.

One of the major changes prompted by the PATRIOT Act revolves around the way government agencies obtain wiretapping authorizations. Previously, police could obtain warrants for only one circuit at a time, after proving that the circuit was used by someone subject to monitoring. Provisions of the PATRIOT Act allow authorities to obtain a blanket authorization for a person and then monitor all communications to or from that person under the single warrant.

Another major change is in the way the government deals with Internet service providers (ISPs). Under the terms of the PATRIOT Act, ISPs may voluntarily provide the government with a large range of information. The PATRIOT Act also allows the government to obtain detailed information on user activity through the use of a subpoena (as opposed to a wiretap).

Finally, the USA PATRIOT Act amends the Computer Fraud and Abuse Act (yes, another set of amendments!) to provide more severe penalties for criminal acts. The PATRIOT Act provides for jail terms of up to 20 years and once again expands the coverage of the CFAA.

Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act (FERPA) is another specialized privacy bill that affects any educational institution that accepts any form of funding from the federal government (the vast majority of schools). It grants certain privacy rights to students older than 18 and the parents of minor students. Specific FERPA protections include the following:

- Parents/students have the right to inspect any educational records maintained by the institution on the student.
- Parents/students have the right to request correction of records they think are erroneous and the right to include a statement in the records contesting anything that is not corrected.
- Schools may not release personal information from student records without written consent, except under certain circumstances.

Identity Theft and Assumption Deterrence Act

In 1998, the president signed the Identity Theft and Assumption Deterrence Act into law. In the past, the only legal victims of identity theft were the creditors who were defrauded. This act makes identity theft a crime against the person whose identity was stolen and provides severe criminal penalties (up to a 15-year prison term and/or a $250,000 fine) for anyone found guilty of violating this law.

Privacy in the Workplace

One of the authors of this book recently had an interesting conversation with a relative who works in an office environment. At a family Christmas party, the author's relative casually mentioned a story he had read online about a local company that had fired several employees for abusing their Internet privileges. He was shocked and couldn't believe that a company would violate their employees' right to privacy.

As you've read in this chapter, the U.S. court system has long upheld the traditional right to privacy as an extension of basic constitutional rights. However, the courts have maintained that a key element of this right is that privacy should be guaranteed only when there is a "reasonable expectation of privacy." For example, if you mail a letter to someone in a sealed envelope, you may reasonably expect that it will be delivered without being read along the way—you have a reasonable expectation of privacy. On the other hand, if you send your message on a postcard, you do so with the awareness that one or more people might read your note before it arrives at the other end—you do not have a reasonable expectation of privacy.

Recent court rulings have found that employees do not have a reasonable expectation of privacy while using employer-owned communications equipment in the workplace. If you send a message using an employer's computer, Internet connection, telephone, or other communications device, your employer can monitor it as a routine business procedure.

That said, if you're planning to monitor the communications of your employees, you should take reasonable precautions to ensure that there is no implied expectation of privacy. Here are some common measures to consider:

- Clauses in employment contracts that state the employee has no expectation of privacy while using corporate equipment
- Similar written statements in corporate acceptable use and privacy policies
- Logon banners warning that all communications are subject to monitoring
- Warning labels on computers and telephones warning of monitoring

> As with many of the issues discussed in this chapter, it's a good idea to consult with your legal counsel before undertaking any communications-monitoring efforts.

European Union Privacy Law

On October 24, 1995, the European Union Parliament passed a sweeping directive outlining privacy measures that must be in place for protecting personal data processed by information systems. The directive went into effect three years later in October 1998. The directive requires that all processing of personal data meet one of the following criteria:

- Consent
- Contract
- Legal obligation
- Vital interest of the data subject
- Balance between the interests of the data holder and the interests of the data subject

The directive also outlines key rights of individuals about whom data is held and/or processed:

- Right to access the data
- Right to know the data's source
- Right to correct inaccurate data
- Right to withhold consent to process data in some situations
- Right of legal action should these rights be violated

American companies doing business in Europe can obtain protection under a treaty between the European Union and the United States that allows the Department of Commerce to certify businesses that comply with regulations and offer them "safe harbor" from prosecution.

To qualify for the safe harbor provision, U.S. companies conducting business in Europe must meet seven requirements for the processing of personal information:

Notice They must inform individuals of what information they collect about them and how the information will be used.

Choice They must allow individuals to opt out if the information will be used for any other purpose or shared with a third party. For information considered sensitive, an opt-in policy must be used.

Onward transfer Organizations can share data only with other organizations that comply with the safe harbor principles.

Access Individuals must be granted access to any records kept containing their personal information.

Security Proper mechanisms must be in place to protect data against loss, misuse, and unauthorized disclosure.

Data Integrity Organizations must take steps to ensure the reliability of the information they maintain.

Enforcement Organizations must make a dispute resolution process available to individuals and provide certifications to regulatory agencies that they comply with the safe harbor provisions.

TIP

For more information on the safe harbor protections available to American companies, visit the Department of Commerce's Safe Harbor website at www.export.gov/safeharbor/.

Investigations

Every information security professional will, at one time or another, encounter a security incident that requires an investigation. In many cases, this investigation will be a brief, informal determination that the matter is not serious enough to warrant further action or the involvement of law enforcement authorities. However, in some cases, the threat posed or damage done will be severe enough to require a more formal inquiry. When this occurs, investigators must be careful to ensure that proper procedures are followed. Failure to abide by the correct procedures may violate the civil rights of those individual(s) being investigated and could result in a failed prosecution or even legal action against the investigator.

Evidence

To successfully prosecute a crime, the prosecuting attorneys must provide sufficient evidence to prove an individual's guilt beyond a reasonable doubt. In the following sections, we'll explain the requirements that evidence must meet before it is allowed in court, the various types of evidence that may be introduced, and the requirements for handling and documenting evidence.

NIST’s Guide to Integrating Forensic Techniques into Incident Response (SP 800-86) is a great reference and available at: www.csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

Admissible Evidence

There are three basic requirements for evidence to be introduced into a court of law. To be considered *admissible evidence*, it must meet all three of these requirements, as determined by the judge, prior to being discussed in open court:

- The evidence must be *relevant* to determining a fact.
- The fact that the evidence seeks to determine must be *material* (that is, related) to the case.
- The evidence must be *competent*, meaning it must have been obtained legally. Evidence that results from an illegal search would be inadmissible because it is not competent.

Types of Evidence

Three types of evidence can be used in a court of law: real evidence, documentary evidence, and testimonial evidence. Each has slightly different additional requirements for admissibility.

Real Evidence

Real evidence (also known as *object evidence*) consists of things that may actually be brought into a court of law. In common criminal proceedings, this may include items such as a murder weapon, clothing, or other physical objects. In a computer crime case, real evidence might include seized computer equipment, such as a keyboard with fingerprints on it or a hard drive from a hacker’s computer system. Depending upon the circumstances, real evidence may also be *conclusive evidence*, such as DNA, that is incontrovertible.

Documentary Evidence

Documentary evidence includes any written items brought into court to prove a fact at hand. This type of evidence must also be authenticated. For example, if an attorney wants to introduce a computer log as evidence, they must bring a witness (for example, the system administrator) into court to testify that the log was collected as a routine business practice and is indeed the actual log that the system collected.

Two additional evidence rules apply specifically to documentary evidence:

- The *best evidence rule* states that, when a document is used as evidence in a court proceeding, the original document must be introduced. Copies or descriptions of original evidence (known as *secondary evidence*) will not be accepted as evidence unless certain exceptions to the rule apply.
- The *parol evidence rule* states that, when an agreement between parties is put into written form, the written document is assumed to contain all the terms of the agreement and no verbal agreements may modify the written agreement.

If documentary evidence meets the materiality, competency, and relevancy requirements and also complies with the best evidence and parol evidence rules, it can be admitted into court.

Chain of Evidence

Real evidence, like any type of evidence, must meet the relevancy, materiality, and competency requirements before being admitted into court. Additionally, real evidence must be authenticated. This can be done by a witness who can actually identify an object as unique (for example, “That knife with my name on the handle is the one that the intruder took off the table in my house and stabbed me with”).

In many cases, it is not possible for a witness to uniquely identify an object in court. In those cases, a *chain of evidence* (also known as a *chain of custody*) must be established. This involves everyone who handles evidence—including the police who originally collect it, the evidence technicians who process it, and the lawyers who use it in court. The location of the evidence must be fully documented from the moment it was collected to the moment it appears in court to ensure that it is indeed the same item. This requires thorough labeling of evidence and comprehensive logs noting who had access to the evidence at specific times and the reasons they required such access.

When evidence is labeled to preserve the chain of custody, the label should include the following types of information regarding the collection:

- General description of the evidence
- Time, date the evidence was collected
- Exact location the evidence was collected from
- Name of the person collecting the evidence
- Relevant circumstances surrounding the collection

Each person who handles the evidence must sign the chain of custody log indicating the time they took direct responsibility for the evidence and the time they handed it off to the next person in the chain of custody. The chain must provide an unbroken sequence of events accounting for the evidence from the time it was collected until the time of the trial.

Testimonial Evidence

Testimonial evidence is, quite simply, evidence consisting of the testimony of a witness, either verbal testimony in court or written testimony in a recorded deposition. Witnesses must take an oath agreeing to tell the truth, and they must have personal knowledge upon which their testimony is based. Furthermore, witnesses must remember the basis for their testimony (they may consult written notes or records to aid their memory). Witnesses can offer *direct evidence*: oral testimony that proves or disproves a claim based upon their own direct observation. The testimonial evidence of most witnesses must be strictly limited to direct evidence based upon the witness's factual observations. However, this does not apply if a witness has been accepted by the court as an expert in a certain field. In that case, the witness may offer an *expert opinion* based upon the other facts presented and their personal knowledge of the field.

Testimonial evidence must not be *hearsay evidence*. That is, a witness cannot testify as to what someone else told them outside court. Computer log files that are not authenticated by a system administrator can also be considered hearsay evidence.

Evidence Collection

Collecting digital evidence is a tricky process and should be attempted only by professional forensic technicians. The International Organization on Computer Evidence (IOCE) outlined six principles to guide digital evidence technicians as they perform media analysis, network analysis, and software analysis in the pursuit of forensically recovered evidence:

- When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Investigation Process

When you initiate a computer security investigation, you should first assemble a team of competent analysts to assist with the investigation.

Calling In Law Enforcement

One of the first decisions that must be made in an investigation is whether law enforcement authorities should be called in. This is actually a relatively complicated decision that should involve senior management officials. There are many factors in favor of calling in the experts. For example, the FBI now maintains a National Computer Crime Squad that includes individuals with the following qualifications:

- Degrees in the computer sciences
- Prior work experience in industry and academic institutions
- Basic and advanced commercial training
- Knowledge of basic data and telecommunications networks

- Experience with Unix and other computer operating systems

On the other hand, two major factors may cause a company to shy away from calling in the authorities. First, the investigation will more than likely become public and may embarrass the company. Second, law enforcement authorities are bound to conduct an investigation that complies with the Fourth Amendment and other legal requirements that may not apply if the organization conducted its own, private investigation.

Search Warrants

Even the most casual viewer of American crime television is familiar with the question, Do you have a warrant? The Fourth Amendment of the U.S. Constitution outlines the burden placed upon investigators to have a valid search warrant before conducting certain searches and the legal hurdle they must overcome to obtain a warrant:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

This amendment contains several important provisions that guide the activities of law enforcement personnel:

- Investigators must obtain a warrant before searching a person's private belongings, assuming that there is a reasonable expectation of privacy. There are a number of documented exceptions to this requirement, such as when an individual consents to a search, the evidence of a crime is in plain view, or there is a life-threatening emergency necessitating the search.
- Warrants can be issued only based upon probable cause. There must be some type of evidence that a crime took place and that the search in question will yield evidence relating to that crime. The standard of "probable cause" required to get a warrant is much weaker than the standard of evidence required to secure a conviction. Most warrants are "sworn out" based solely upon the testimony of investigators.
- Warrants must be specific in their scope. The warrant must contain a detailed description of the legal bounds of the search and seizure.

If investigators fail to comply with even the smallest detail of these provisions, they may find their warrant invalidated and the results of the search deemed inadmissible. This leads to another one of those American colloquialisms: “He got off on a technicality.”

Conducting the Investigation

If you elect not to call in law enforcement, you should still attempt to abide by the principles of a sound investigation to ensure the accuracy and fairness of your inquiry. It is important to remember a few key principles:

- Never conduct your investigation on an actual system that was compromised. Take the system offline, make a backup, and use the backup to investigate the incident.
- Never attempt to “hack back” and avenge a crime. You may inadvertently attack an innocent third party and find yourself liable for computer crime charges.
- If in doubt, call in expert assistance. If you don’t want to call in law enforcement, contact a private investigations firm with specific experience in the field of computer security investigations.
- Usually, it’s best to begin the investigation process using informal interviewing techniques. These are used to gather facts and determine the substance of the case. When specific suspects are identified, they should be questioned using interrogation techniques. Interviewing typically involves open-ended questions to gather information. Interrogation often involves closed-ended questioning with a specific goal in mind and is more adversarial in nature. Again, this is an area best left untouched without specific legal advice.

Summary

Computer security necessarily entails a high degree of involvement from the legal community. In this chapter, you learned about a large number of laws that govern security issues such as computer crime, intellectual property, data privacy, and software licensing. You also learned about the procedures that must be followed when investigating an incident and collecting evidence that may later be admitted into a court of law during a civil or criminal trial.

Granted, computer security professionals cannot be expected to understand the intricate details of all of the laws that cover computer security. However, the main objective of this chapter is to provide you with the foundations of that knowledge. The best legal skill that a CISSP candidate should have is ability to identify a legally questionable issue and know when to call in an attorney who specializes in computer/Internet law.

Exam Essentials

Understand the differences between criminal law, civil law, and administrative law. Criminal law protects society against acts that violate the basic principles we believe in. Violations of criminal law are prosecuted by federal and state governments. Civil law provides the framework for the transaction of business between people and organizations. Violations of civil law are brought to the court and argued by the two affected parties. Administrative law is used by government agencies to effectively carry out their day-to-day business.

Be able to explain the basic provisions of the major laws designed to protect society against computer crime. The Computer Fraud and Abuse Act (as amended) protects computers used by the government or in interstate commerce from a variety of abuses. The Computer Security Act outlines steps the government must take to protect its own systems from attack. The Government Information Security Reform Act further develops the federal government information security program.

Know the difference between copyrights, trademarks, patents, and trade secrets. Copyrights protect original works of authorship, such as books, articles, poems, and songs. Trademarks are names, slogans, and logos that identify a company, product, or service. Patents provide protection to the creators of new inventions. Trade secret law protects the operating secrets of a firm.

Be able to explain the basic provisions of the Digital Millennium Copyright Act of 1998. The Digital Millennium Copyright Act prohibits the circumvention of copy protection mechanisms placed in digital media and limits the liability of Internet service providers for the activities of their users.

Know the basic provisions of the Economic Espionage Act of 1996. The Economic Espionage Act provides penalties for individuals found guilty of the theft of trade secrets. Harsher penalties apply when the individual knows that the information will benefit a foreign government.

Understand the various types of software license agreements. Contractual license agreements are written agreements between a software vendor and user. Shrink-wrap agreements are written on software packaging and take effect when a user opens the package. Click-wrap agreements are included in a package but require the user to accept the terms during the software installation process.

Explain the impact of the Uniform Computer Information Transactions Act on software licensing. The Uniform Computer Information Transactions Act provides a framework for the enforcement of shrink-wrap and click-wrap agreements by federal and state governments.

Understand the restrictions placed upon export of high-performance hardware and encryption technology outside the United States. No high-performance computers or encryption technology may be exported to Tier 4 countries. The export of hardware capable of operating in excess of 0.75 weighted teraflops to Tier 3 countries must be approved by the Department of Commerce. New rules permit the easy exporting of "mass market" encryption software.

Understand the major laws that govern privacy of personal information in both the United States and the European Union. The United States has a number of privacy laws that affect the government's use of information as well as the use of information by specific industries, such as financial services companies and health-care organizations that handle sensitive information. The European Union has a more comprehensive directive on data privacy that regulates the use and exchange of personal information.

Know the basic requirements for evidence to be admissible in a court of law. To be admissible, evidence must be relevant to a fact at issue in the case, the fact must be material to the case, and the evidence must be competent, or legally collected.

Explain the various types of evidence that may be used in a criminal or civil trial. Real evidence consists of actual objects that can be brought into the courtroom. Documentary evidence consists of written documents that provide insight into the facts. Testimonial evidence consists of verbal or written statements made by witnesses.

Written Lab

1. What are the key rights guaranteed to individuals under the European Union’s directive on data privacy?

2. What are the three basic requirements that evidence must meet in order to be admissible in court?

3. What are some common steps that employers take to notify employees of system monitoring?

Answers to Written Lab

1. Individuals have a right to access records kept about them and know the source of data included in those records. They also have the right to correct inaccurate records. Individuals have the right to withhold consent from data processors and have legal recourse if these rights are violated.

2. To be admissible, evidence must be reliable, competent, and material to the case.

3. Some common steps that employers take to notify employees of monitoring include clauses in employment contracts that state the employee should have no expectation of privacy while using corporate equipment, similar written statements in corporate acceptable use and privacy policies, logon banners warning that all communications are subject to monitoring, and labels on computers and telephones warning of monitoring.

Review Questions

1. Which criminal law was the first to implement penalties for the creators of viruses, worms, and other types of malicious code that cause harm to computer system(s)?

A. Computer Security Act

B. National Infrastructure Protection Act

C. Computer Fraud and Abuse Act

D. Electronic Communications Privacy Act

2. Which law first required operators of federal interest computer systems to undergo periodic training in computer security issues?

A. Computer Security Act

B. National Infrastructure Protection Act

C. Computer Fraud and Abuse Act

D. Electronic Communications Privacy Act

3. What type of law does not require an act of Congress to implement at the federal level but, rather, is enacted by the executive branch in the form of regulations, policies, and procedures?

A. Criminal law

B. Common law

C. Civil law

D. Administrative law

4. Which federal government agency has responsibility for ensuring the security of government computer systems that are not used to process sensitive and/or classified information?

A. National Security Agency

B. Federal Bureau of Investigation

C. National Institute of Standards and Technology

D. Secret Service

5. What is the broadest category of computer systems protected by the Computer Fraud and Abuse Act, as amended?

A. Government-owned systems

B. Federal interest systems

C. Systems used in interstate commerce

D. Systems located in the United States

6. What law protects the right of citizens to privacy by placing restrictions on the authority granted to government agencies to search private residences and facilities?

A. Privacy Act

B. Fourth Amendment

C. Second Amendment

D. Gramm-Leach-Bliley Act

7. Matthew recently authored an innovative algorithm for solving a mathematical problem, and he wants to share it with the world. However, prior to publishing the software code in a technical journal, he wants to obtain some sort of intellectual property protection. Which type of protection is best suited to his needs?

A. Copyright

B. Trademark

C. Patent

D. Trade secret

8. Mary is the cofounder of Acme Widgets, a manufacturing firm. Together with her partner, Joe, she has developed a special oil that will dramatically improve the widget manufacturing process. To keep the formula secret, Mary and Joe plan to make large quantities of the oil by themselves in the plant after the other workers have left. They want to protect this formula for as long as possible. What type of intellectual property protection best suits their needs?

A. Copyright

B. Trademark

C. Patent

D. Trade secret

9. Richard recently developed a great name for a new product that he plans to begin using immediately. He spoke with his attorney and filed the appropriate application to protect his product name but has not yet received a response from the government regarding his application. He wants to begin using the name immediately. What symbol should he use next to the name to indicate its protected status?

A. ©

B. ®

C. ™

D. †

10. What law prevents government agencies from disclosing personal information that an individual supplies to the government under protected circumstances?

A. Privacy Act

B. Electronic Communications Privacy Act

C. Health Insurance Portability and Accountability Act

D. Gramm-Leach-Bliley Act

11. What law formalizes many licensing arrangements used by the software industry and attempts to standardize their use from state to state?

A. Computer Security Act

B. Uniform Computer Information Transactions Act

C. Digital Millennium Copyright Act

D. Gramm-Leach-Bliley Act

12. The Children’s Online Privacy Protection Act was designed to protect the privacy of children using the Internet. What is the minimum age a child must be before companies can collect personal identifying information from them without parental consent?

A. 13

B. 14

C. 15

D. 16

13. Which one of the following is not a requirement that Internet service providers must satisfy in order to gain protection under the "transitory activities" clause of the Digital Millennium Copyright Act?

A. The service provider and the originator of the message must be located in different states.

B. The transmission, routing, provision of connections, or copying must be carried out by an automated technical process without selection of material by the service provider.

C. Any intermediate copies must not ordinarily be accessible to anyone other than anticipated recipients and must not be retained for longer than reasonably necessary.

D. The transmission must be originated by a person other than the provider.

14. Which one of the following laws is not designed to protect the privacy rights of consumers and Internet users?

A. Health Insurance Portability and Accountability Act

B. Identity Theft Assumption and Deterrence Act

C. USA PATRIOT Act

D. Gramm-Leach-Bliley Act

15. Which one of the following types of licensing agreements does not require that the user acknowledge that they have read the agreement prior to executing it?

A. Standard license agreement

B. Shrink-wrap agreement

C. Click-wrap agreement

D. Verbal agreement

16. What industry is most directly impacted by the provisions of the Gramm-Leach-Bliley Act?

A. Health care

B. Banking

C. Law enforcement

D. Defense contractors

17. What is the standard duration of patent protection in the United States?

A. 14 years from the application date

B. 14 years from the date the patent is granted

C. 20 years from the application date

D. 20 years from the date the patent is granted

18. Which one of the following is not a valid legal reason for processing information about an individual under the European Union's data privacy directive?

A. Contract

B. Legal obligation

C. Marketing needs

D. Consent

19. What type of evidence must be authenticated by a witness who can uniquely identify it or through a documented chain of custody?

A. Documentary evidence

B. Testimonial evidence

C. Real evidence

D. Hearsay evidence

20. What evidentiary principle states that a written contract is assumed to contain all the terms of an agreement?

A. Material evidence

B. Best evidence

C. Parol evidence

D. Relevant evidence

Answers to Review Questions

1. C. The Computer Fraud and Abuse Act, as amended, provides criminal and civil penalties for those individuals convicted of using viruses, worms, Trojan horses, and other types of malicious code to cause damage to computer system(s).

2. A. The Computer Security Act requires mandatory periodic training for all people involved in managing, using, or operating federal computer systems that contain sensitive information.

3. D. Administrative laws do not require an act of the legislative branch to implement at the federal level. Administrative laws consist of the policies, procedures, and regulations promulgated by agencies of the executive branch of government. Although they do not require an act of Congress, these laws are subject to judicial review and must comply with criminal and civil laws enacted by the legislative branch.

4. C. The National Institute of Standards and Technology (NIST) is charged with the security management of all federal government computer systems that are not used to process sensitive national security information. The National Security Agency (part of the Department of Defense) is responsible for managing those systems that do process classified and/or sensitive information.

5. C. The original Computer Fraud and Abuse Act of 1984 covered only systems used by the government and financial institutions. The act was broadened in 1986 to include all federal interest systems. The Computer Abuse Amendments Act of 1994 further amended the CFAA to cover all systems that are used in interstate commerce, covering a large portion (but not all) of the computer systems in the United States.

6. B. The Fourth Amendment to the U.S. Constitution sets the “probable cause” standard that law enforcement officers must follow when conducting searches and/or seizures of private property. It also states that those officers must obtain a warrant before gaining involuntary access to such property.

7. A. Copyright law is the only type of intellectual property protection available to Matthew. It covers only the specific software code that Matthew used. It does not cover the process or ideas behind the software.

Trademark protection is not appropriate for this type of situation. Patent protection does not apply to mathematical algorithms. Matthew can't seek trade secret protection because he plans to publish the algorithm in a public technical journal.

8. D. Mary and Joe should treat their oil formula as a trade secret. As long as they do not publicly disclose the formula, they can keep it a company secret indefinitely.

9. C. Richard's product name should be protected under trademark law. Until his registration is granted, he can use the ™ symbol next to it to inform others that it is protected under trademark law. Once his application is approved, the name becomes a registered trademark and Richard can begin using the ® symbol.

10. A. The Privacy Act of 1974 limits the ways government agencies may use information that private citizens disclose to them under certain circumstances.

11. B. The Uniform Computer Information Transactions Act (UCITA) attempts to implement a standard framework of laws regarding computer transactions to be adopted by all states. One of the issues addressed by UCITA is the legality of various types of software license agreements.

12. A. The Children's Online Privacy Protection Act (COPPA) provides severe penalties for companies that collect information from young children without parental consent. COPPA states that this consent must be obtained from the parents of children younger than the age of 13 before any information is collected (other than basic information required to obtain that consent).

13. A. The Digital Millennium Copyright Act does not include any geographical location requirements for protection under the "transitory activities" exemption. The other options are three of the five mandatory requirements. The other two requirements are that the service provider must not determine the recipients of the material and the material must be transmitted with no modification to its content.

14. C. The USA PATRIOT Act was adopted in the wake of the September 11, 2001, terrorist attacks. It broadens the powers of the government to monitor communications between private citizens and therefore actually weakens the privacy rights of consumers and Internet users. The other laws mentioned all contain provisions designed to enhance individual privacy rights.

15. B. Shrink-wrap license agreements become effective when the user opens a software package. Click-wrap agreements require the user to click a button during the installation process to accept the terms of the license agreement. Standard license agreements require that the user sign a written agreement prior to using the software. Verbal agreements are not normally used for software licensing but also require some active degree of participation by the software user.

16. B. The Gramm-Leach-Bliley Act provides, among other things, regulations regarding the way financial institutions can handle private information belonging to their customers.

17. C. U.S. patent law provides for an exclusivity period of 20 years beginning at the time the patent application is submitted to the Patent and Trademark Office.

18. C. Marketing needs are not a valid reason for processing personal information, as defined by the European Union privacy directive.

19. C. Real evidence must be either uniquely identified by a witness or authenticated through a documented chain of custody.

20. C. The parol evidence rule states that a written contract is assumed to contain all the terms of an agreement and cannot be modified by a verbal agreement.

Chapter 18

Incidents and Ethics

THE CISSP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

- **Information Security Governance and Risk Management**
    - Understand professional ethics
        - (ISC)^2 code of professional ethics; support organization's code of ethics
- **Legal, Regulations, Investigations, and Compliance**
    - Understand legal issues that pertain to information security internationally
        - Computer crime; licensing and intellectual property (e.g., copyright, trademark); import/export; trans-border data flow; privacy
    - Understand and support investigations
        - Policy; incident handling and response; evidence collection and handling (e.g., chain of custody, interviewing); reporting and documenting
    - Understand forensic procedures
        - Media analysis; network analysis; software analysis
    - Understand compliance requirements and procedures
        - Regulatory environment; audits; reporting
- **Operations Security**
    - Manage incident response
        - Detection; response; reporting; recovery; remediation

In this chapter, we'll continue our discussion from Chapter 17, "Law and Investigations," regarding the Legal Regulations, Investigations, and Compliance domain of the Common Body of Knowledge (CBK) for the CISSP certification exam. This domain deals with topics and issues related to computer crime laws and regulations, investigative techniques used to determine whether a computer crime has been committed and to collect evidence when appropriate, and ethics issues and code of conduct for the information security practitioner.

The first step in deciding how to respond to a computer attack is to know if and when an attack has taken place. You must know how to determine that an attack is occurring, or has occurred, before you can properly choose a course of action. Once you have determined that an incident has occurred, the next step is to conduct an investigation and collect evidence to find out what has happened and determine the extent of any damage that might have been done. You must be sure you conduct the investigation in accordance with local laws and regulations.

Major Categories of Computer Crime

There are many ways to attack a computer system and many motivations to do so. Information system security practitioners generally put crimes against or involving computers into different categories. Simply put, a *computer crime* is a crime (or violation of a law or regulation) that involves a computer. The crime could be against the computer, or the computer could have been used in the actual commission of the crime. Each of the categories of computer crimes represents the purpose of an attack and its intended result.

Any individual who violates one or more of your security policies is considered to be an *attacker*. An attacker uses different techniques to achieve a specific goal. Understanding the goals helps to clarify the different types of attacks. Remember that crime is crime, and the motivations behind computer crime are no different from the motivations behind any other type of crime. The only real difference may be in the methods the attacker uses to strike.

Computer crimes are generally classified as one of the following types:

- Military and intelligence attacks
- Business attacks
- Financial attacks
- Terrorist attacks
- Grudge attacks
- Thrill attacks

It is important to understand the differences among the categories of computer crime to best understand how to protect a system and react when an attack occurs. The type and amount of evidence left by an attacker is often dependent on their expertise. In the following sections, we’ll discuss the different categories of computer crimes and the types of evidence you might find after an attack. This evidence can help you determine the attacker's actions and intended target. You may find that your system was only a link in the chain of network hops used to reach the real victim, making the trail harder to follow back to the true attacker.

Military and Intelligence Attacks

Military and intelligence attacks are launched primarily to obtain secret and restricted information from law enforcement or military and technological research sources. The disclosure of such information could compromise investigations, disrupt military planning, and threaten national security. Attacks to gather military information or other sensitive intelligence often precede other, more damaging attacks.

An attacker may be looking for the following kinds of information:

- Military descriptive information of any type, including deployment information, readiness information, and order of battle plans
- Secret intelligence gathered for military or law enforcement purposes
- Descriptions and storage locations of evidence obtained in a criminal investigation
- Any secret information that could be used in a later attack

Because of the sensitive nature of information collected and used by the military and intelligence agencies, their computer systems are often attractive targets for experienced attackers. To protect from more numerous and more sophisticated attackers, you will generally find more formal security policies in place on systems that house such information. As you learned in Chapter 5, "Security Management Concepts and Principles," data can be classified according to sensitivity and stored on systems that support the required level of security. It is common to find stringent perimeter security as well as internal controls to limit access to classified documents on military and intelligence agency systems.

You can be sure that serious attacks to acquire military or intelligence information are carried out by professionals. Professional attackers are generally very thorough in covering their tracks. There is usually very little evidence to collect after such an attack. Attackers in this category are the most successful and the most satisfied when no one is aware that an attack occurred.

Business Attacks

Business attacks focus on illegally obtaining an organization’s confidential information. This could be information that is critical to the operation of the organization, such as a secret recipe, or information that could damage the organization’s reputation if disclosed, such as personal information about its employees. The gathering of a competitor’s confidential information, also called *industrial espionage*, is not a new phenomenon. Businesses have used illegal means to acquire competitive information for many years. The temptation to steal a competitor’s trade secrets and the ease with which a savvy attacker can compromise some computer systems makes this type of attack attractive.

The goal of business attacks is solely to extract confidential information. The use of the information gathered during the attack usually causes more damage than the attack itself. A business that has suffered an attack of this type can be put into a position from which it might not ever recover. It is up to you as the security professional to ensure that the systems that contain confidential data are secure. In addition, a policy must be developed that will handle such an intrusion should it occur. (For more information on security policies, see Chapter 6, “Asset Value, Policies, and Roles.”)

Financial Attacks

Financial attacks are carried out to unlawfully obtain money or services. They are the type of computer crime you most commonly hear about in the news. The goal of a financial attack could be to steal credit card numbers, increase the balance in a bank account, or place “free” long-distance telephone calls. You have probably heard of individuals breaking into telephone company computers and placing free calls. This type of financial attack is called *phone phreaking*.

Shoplifting and burglary are both examples of financial attacks. You can usually tell the sophistication of the attacker by the dollar amount of the damages. Less-sophisticated attackers seek easier targets, but although the damages are usually minimal, they can add up over time.

Financial attacks launched by sophisticated attackers can result in substantial damages. Although phone phreaking causes the telephone company to lose the revenue of calls placed, serious financial attacks can result in losses amounting to millions of dollars. As with the attacks previously described, the ease with which you can detect an attack and track an attacker is largely dependent on the attacker's skill level.

Terrorist Attacks

Terrorist attacks are a reality in modern society. Our increasing reliance upon information systems makes them more and more attractive to terrorists. Such attacks differ from military and intelligence attacks. The purpose of a terrorist attack is to disrupt normal life and instill fear, whereas a military or intelligence attack is designed to extract secret information. Intelligence gathering generally precedes any type of terrorist attack. The very systems that are victims of a terrorist attack were probably compromised in an earlier attack to collect intelligence. The more diligent you are in detecting attacks of any type, the better prepared you will be to intervene before more serious attacks occur.

Possible targets of a computer terrorist attack could be systems that regulate power plants or control telecommunications or power distribution. Many such control and regulatory systems are computerized and vulnerable to terrorist action. In fact, the possibility exists of a simultaneous physical and computerized terrorist attack. Our ability to respond to such an attack would be greatly diminished if the physical attack were simultaneously launched with a computer attack designed to knock out power and communications.

Most large power and communications companies have dedicated a security staff to ensure the security of their systems, but many smaller businesses that have systems connected to the Internet are more vulnerable to attacks. You must diligently monitor your systems to identify any attacks and then respond swiftly when an attack is discovered.

Grudge Attacks

Grudge attacks are attacks that are carried out to damage an organization or a person. The damage could be in the loss of information or information processing capabilities or harm to the organization or a person's reputation.

The motivation behind a grudge attack is usually a feeling of resentment, and the attacker could be a current or former employee or someone who wishes ill will upon an organization. The attacker is disgruntled with the victim and takes out their frustration in the form of a grudge attack.

An employee who has recently been fired is a prime example of a person who might carry out a grudge attack to "get back" at the organization. Another example is a person who has been rejected in a personal relationship with another employee. The person who has been rejected might launch an attack to destroy data on the victim's system.

Real World Scenario

The Insider Threat

It's common for security professionals to focus on the threat from outside an organization. Indeed, many of our security technologies are designed to keep unauthorized individuals out. We often don't pay enough (or much!) attention to protecting our organizations against the malicious insider, even though they often pose the greatest risk to our computing assets.

One of the authors of this book recently wrapped up a consulting engagement with a medium-sized subsidiary of a large, well-known corporation. The company had suffered a serious security breach, involving the theft of thousands of dollars and the deliberate destruction of sensitive corporate information. The IT leaders within the organization needed someone to work with them to diagnose the cause of the event and protect themselves against similar events in the future.

After only a very small amount of digging, it became apparent that they were dealing with an insider attack. The intruder's actions demonstrated knowledge of the company's IT infrastructure as well as an understanding of which data was most important to the company's ongoing operations.

Additional investigation revealed that the culprit was a former employee who ended his employment with the firm on less-than-favorable terms. He left the building with a chip on his shoulder and an ax to grind. Unfortunately, he was a system administrator with a wide range of access to corporate systems, and the company had an immature deprovisioning process that failed to remove all of his access upon his termination. He simply found several accounts that remained active and used them to access the corporate network through a VPN.

The moral of this story? Don't underestimate the insider threat. Take the time to evaluate your controls to mitigate the risk that malicious current and former employees pose to your organization.

Your security policy should address the potential of attacks by disgruntled employees. For example, as soon as an employee is terminated, all system access for that employee should be terminated. This action reduces the likelihood of a grudge attack and removes unused access accounts that could be used in future attacks.

Although most grudge attackers are just disgruntled people with limited hacking and cracking abilities, some possess the skills to cause substantial damage. An unhappy cracker can be a handful for security professionals. Take extreme care when a person with known cracking ability leaves your company. At the least, you should perform a vulnerability assessment of all systems the person could access. You may be surprised to find one or more "back doors" left in the system. (For more on back doors, see Chapter 8, "Malicious Code and Application Attacks.") But even in the absence of any back doors, a former employee who is familiar with the technical architecture of the organization may know how to exploit its weaknesses.

Grudge attacks can be devastating if allowed to occur unchecked. Diligent monitoring and assessing systems for vulnerabilities is the best protection for most grudge attacks.

Thrill Attacks

Thrill attacks are the attacks launched only for the fun of it. Attackers who lack the ability to devise their own attacks will often download programs that do their work for them. These attackers are often called *script kiddies* because they run only other people's programs, or scripts, to launch an attack.

The main motivation behind these attacks is the "high" of successfully breaking into a system. If you are the victim of a thrill attack, the most common fate you will suffer is a service interruption. Although an attacker of this type may destroy data, the main motivation is to compromise a system and perhaps use it to launch an attack against another victim.

One common type of thrill attack involves website defacements, where the attacker compromises a web server and replaces an organization's legitimate web content with other pages, often boasting about the attacker's skills. For example, an attacker operating under the pseudonym iSKORPiTX conducted more than 20,000 website defacements in 2006, replacing legitimate websites with his own pages containing the text "Hacked by iSKORPiTX."

Evidence

Chapter 17 included general coverage of the topic of evidence. Remember that the term *evidence* refers to any hardware, software, or data that you can use to prove the identity and actions of an attacker. It's extremely important that you properly handle any and all evidence you collect after an attack, especially if you intend to use the information in court proceedings. You should realize that most computer evidence is intangible, meaning it is electronic and magnetically stored information that is vulnerable to erasure, corruption, and other forms of damage.

Your ability to recover damages in a court of law may depend solely on your diligence during the evidence collection process. In fact, your ability to determine the extent of an attack depends on your evidence collecting abilities. Once an attack has been identified, you should start the evidence collection process. Always assume an attack will result in a legal battle. It is far easier to take evidence collection seriously from the beginning than to later realize an attack was more severe than first thought and then try to go back and do it right. Following standard evidence collection procedures also ensures that you conduct your investigation in an orderly, scientific manner.

In most attacks, evidence of some kind is left. However, professional attackers may leave evidence that is so subtle that it is difficult or impossible to find. Another problem with evidence is that it is often time sensitive. Your logs probably roll over periodically and old information is lost. Do you know the frequency of your log purge routines? Some attacks leave traces in memory. The bulk of the evidence will be lost when you remove power from the system. Each step you take as you collect evidence should be deliberate and well documented.

You must know what your system baseline looks like and how it operates in a normal mode. Without this knowledge, you will be hard-pressed to recognize an attack or to know where to search for valuable evidence. Experienced security professionals learn how their systems operate on a daily basis and are comfortable with the regular operations of the system. The more you understand the “normal” state of your systems, the more an unusual event will stand out.

Incident Handling

When an incident occurs, you must handle it in a manner that is outlined in your security policy and consistent with local laws and regulations. The first step in handling an incident properly is recognizing when one occurs. You should understand the following two terms related to incident handling:

Event Any occurrence that takes place during a certain period of time

Incident An event that has a negative outcome affecting the confidentiality, integrity, or availability of an organization’s data

The most common reason incidents are not reported is that they are never identified. You could have many security policy violations occurring each day, but if you don’t have a way of identifying them, you will never know. Therefore, your security policy should identify and list all possible violations and ways to detect them. It’s also important to update your security policy as new types of violations and attacks emerge.

What you do when you find that an incident has occurred depends on the type of incident and scope of damage. Law dictates that some incidents must be reported, such as those that impact government or federal interest computers (a federal interest computer is one that is used by financial institutions and by infrastructure systems such as water and power systems) or certain financial transactions, regardless of the amount of damage. Most U.S. states now have laws that require organizations that experience an incident involving certain types of personally identifying information (for example, credit card numbers, Social Security numbers, and driver's license numbers) to notify affected individuals of the breach.

In addition to laws, many companies have contractual obligations to report different types of security incidents to business partners. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires any merchant that handles credit card information to report incidents involving that information to their acquiring bank as well as law enforcement.

Next, we'll cover some of the different types of incidents and typical responses.

Common Types of Incidents

We discussed the different types of attacks in Chapter 2, "Attacks and Monitoring." An incident occurs when an attack, or other violation of your security policy, is carried out against your system. There are many ways to classify incidents; here is a general list of categories:

- Scanning
- Compromises
- Malicious code
- Denial of service

These four areas are the basic entry points for attackers to impact a system. You must focus on each of these areas to create an effective monitoring strategy that detects system incidents. Each incident area has representative signatures that can tip off an alert security administrator that an incident has occurred. Make sure you know your operating system environment and where to look for the telltale signs of each type of incident.

Scanning

Scanning attacks are reconnaissance attacks that usually precede another, more serious attack. They're comparable to a burglar "casing" a neighborhood for targets, looking for homes with unlocked doors or where nobody is home on guard. Attackers will gather as much information about your system as possible before launching a directed attack. Look for any unusual activity on any port or from any single address. For example, a high volume of Secure Shell (SSH) packets on port 22 may point to a systematic scan of your network.

Remember that simply scanning your system may not be illegal, depending upon your local laws. It can indicate that illegal activity will follow, so it is a good idea to treat scans as incidents and to collect evidence of scanning activity. You may find that the evidence you collect at the time the system is scanned could be the link you need later to find the party responsible for a later attack.

Because scanning is such a common occurrence, you definitely want to automate evidence collection. Set up your firewall to log rejected traffic and archive your log files. The logs may become large, but storage is cheap, and you should consider it a cost of doing business.

Compromise

A system *compromise* is any unauthorized access to the system or information the system stores. A compromise could originate inside or outside the organization. To make matters worse, a compromise could come from a valid user. An unauthorized use of a valid user ID is just as much of a compromise incident as an experienced cracker breaking in from the outside. Another example of a system compromise is when an attacker uses a normal user account to gain the elevated privileges of a system administrator without authorization.

System compromises can be very difficult to detect. Most often, the data custodian notices something unusual about the data. It could be missing, altered, or moved; the time stamps could be different; or something else is just not right. The more you know about the normal operation of your system, the better prepared you will be to detect abnormal system behavior.

Malicious Code

When *malicious code* is mentioned, you probably think of viruses and spyware. Although a virus is a common type of malicious code, it is only one type of several. (In Chapter 8, we discussed different types of malicious code.) Detection of this type of a malicious code incident comes from either an end user reporting behavior caused by the malicious code or an automated alert reporting that scanned code containing a malicious component has been found.

The most effective way to protect your system from malicious code is to implement virus and spyware scanners and keep the signature database up-to-date. In addition, your security policy should address the introduction of outside code. Be specific as to what code you will allow end users to install.

Denial of Service

The final type of incident is a *denial of service (DoS)*. This type of incident is often the easiest to detect. A user or automated tool reports that one or more services (or the entire machine) is unavailable. Although they're simple to detect, avoidance is a far better course of action. It is theoretically possible to dynamically alter firewall rules to reject DoS network traffic, but in recent years the sophistication and complexity of DoS attacks make them extremely difficult to defend against. Because there are so many variations of the DoS attack, implementing this strategy is a nontrivial task.

A detailed discussion of DoS and distributed denial-of-service (DDoS) attacks appears in Chapter 8.

Response Teams

Many organizations now have a dedicated team responsible for investigating any computer security incidents that take place. These teams are commonly known as computer incident response teams (CIRTs) or computer security incident response teams (CSIRTs). When an incident occurs, the response team has four primary responsibilities:

- Determine the amount and scope of damage caused by the incident.
- Determine whether any confidential information was compromised during the incident.
- Implement any necessary recovery procedures to restore security and recover from incident-related damages.
- Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.

Real World Scenario

The Gibson Research Denial-of-Service Attacks: Fun or Grudge?

Steve Gibson is a well-known software developer and personality in the IT industry whose high visibility derives not only from highly regarded products associated with his company, Gibson Research, but also from his many years as a vocal and outspoken columnist for *Computer World* magazine. In recent years, he has become quite active in the field of computer security, and his site offers free vulnerability-scanning services and a variety of patches and fixes for operating system vulnerabilities. He operates a website at http://grc.comthat has been the subject of numerous well-documented denial-of-service attacks. It's interesting to speculate whether such attacks are motivated by grudges (that is, by those who seek to advance their reputations by breaking into an obvious and presumably well-defended point of attack) or by fun (that is, by those with excess time on their hands who might seek to prove themselves against a worthy adversary without necessarily expecting any gain other than notoriety from their actions).

Gibson's website has in fact been subject to two well-documented denial-of-service attacks that you can read about in detail on his site:

- "Distributed Reflection Denial of Service": www.dsinet.org/files/textfiles/tcp-ip/Distributed%20Reflection%20Denial%20of%20Service.pdf
- "The Strange Tale of the Denial of Service Attacks against GRC.COM": www.crime-research.org/library/grcdos.pdf

Although his subsequent anonymous discussions with one of the perpetrators involved seem to indicate that the motive for some of these attacks was fun rather than business damage or acting on a grudge, these reports are fascinating because of the excellent model they provide for incident handling and reporting.

These documents contain a brief synopsis of the symptoms and chronology of the attacks that occurred, along with short- and long-term fixes and changes enacted to prevent recurrences. They also stress the critical importance of communication with service providers whose infrastructures may be involved in attacks as they're underway. What's extremely telling about Gibson's report on the denial-of-service attacks is that he experienced 17 hours of downtime because he was unable to establish contact with a knowledgeable, competent engineer at his service provider who could help define the right kinds of traffic filters to stymie the floods of traffic that characterize denial-of-service attacks.

Gibson’s analysis also indicates his thoroughness in analyzing the sources of the distributed denial-of-service attacks and in documenting what he calls “an exact profile of the malicious traffic being generated during these attacks.” This information permitted his ISP to define a set of filters that blocked further such traffic from transiting the final T1 links from Gibson’s Internet service provider to his servers. As his experience proves so conclusively, recognizing, analyzing, and characterizing attacks is absolutely essential to defining filters or other countermeasures that can block or defeat them.

As part of these duties, the team should facilitate a *postmortem review* of the incident within a week of the occurrence to ensure that key players in the incident share their knowledge and develop best practices to assist in future incident response efforts.

When putting together your incident response team, be sure to design a cross-functional group of individuals that represent the management, technical, and functional areas of responsibility most directly impacted by a security incident. Potential team members include the following:

- Representative of senior management
- Information security professionals
- Legal representatives
- Public affairs/communications representatives
- Engineering representatives (system and network)

Incident Response Process

Many organizations use a three-step incident response process, consisting of the following phases:

1. Detection and identification

2. Response and reporting

3. Recovery and remediation

The next three sections outline each phase of the standard incident response process.

Step 1: Detection and Identification

The incident identification process has two main goals: identifying incidents and notifying appropriate personnel. To successfully detect and identify incidents, a security team must monitor any relevant events that occur and notice when they meet the organization's defined threshold for a security incident. The key to identifying incidents is to detect abnormal or suspicious activity that may constitute evidence of an incident. Although you can detect many attacks by their characteristic signatures, experienced attackers know how to "fly under the radar." You must be very aware of how your system operates normally. *Abnormal* or *suspicious* activity is any system activity that does not normally occur on your system.

These are some of the tools and techniques you should monitor for events indicative of security incidents:

- Intrusion detection/prevention systems
- Antivirus software
- Firewall logs
- System logs
- Physical security systems
- File integrity monitoring software

Always use multiple sources of data when investigating an incident. Be suspicious of anything that does not make sense. Ensure that you can clearly explain any activity you see that is not normal for your system. If it just does not "feel" right, it could be the only clue you have to successfully intervene in an ongoing incident.

Once the initial evaluator identifies that an event or events meet the organization's security incident criteria, the evaluator must notify the incident response team. This notification concludes the incident detection and identification phase and initiates the response and reporting phase.

Step 2: Response and Reporting

Once you determine that an incident has occurred, the next step is to choose an appropriate response. Your security policy should specify steps to take for various types of incidents. Always proceed with the assumption that an incident will end up in a court of law. Treat any evidence you collect as if it must pass admissibility standards. Once you taint evidence, there is no going back. You must ensure that the chain of evidence is maintained.

Isolation and Containment

The first actions you take should be dedicated to limiting the exposure of your organization and preventing further damage. In the case of a potentially compromised system, you should disconnect it from the network to prevent intruders from accessing the compromised system and also to prevent the compromised system from affecting other resources on the network.

WARNING

> In the isolation and containment phase of incident response, it is critical that you leave the system in a running state. Do not power down the system. Turning off the computer destroys the contents of volatile memory and may destroy evidence.

Gathering Evidence

It is common to confiscate equipment, software, or data to perform a proper investigation. The manner in which the evidence is confiscated is important. The confiscation of evidence must be carried out in a proper fashion. There are three basic alternatives.

First, the person who owns the evidence could *voluntarily surrender* it. This method is generally appropriate only when the attacker is not the owner. Few guilty parties willingly surrender evidence they know will incriminate them. Less-experienced attackers may believe they have successfully covered their tracks and voluntarily surrender important evidence. A good forensic investigator can extract much “covered-up” information from a computer. In most cases, asking for evidence from a suspected attacker just alerts the suspect that you are close to taking legal action.

TIP

> In the case of an internal investigation, you will gather the vast majority of your information through voluntary surrender. Most likely, you’re conducting the investigation under the auspices of a senior member of management who will authorize you to access any organizational resources necessary to complete your investigation.

Second, you could get a court to issue a *subpoena*, or court order, that compels an individual or organization to surrender evidence and then have the subpoena served by law enforcement. Again, this course of action provides sufficient notice for someone to alter the evidence and render it useless in court.

The last option is a *search warrant*. This option should be used only when you must have access to evidence without tipping off the evidence’s owner or other personnel. You must have a strong suspicion with credible reasoning to convince a judge to pursue this course of action.

The three alternatives apply to confiscating equipment both inside and outside an organization, but there is another step you can take to ensure that the confiscation of equipment that belongs to your organization is carried out properly. It is common to have all new employees sign an agreement that provides consent to search and seize any necessary evidence during an investigation. In this manner, consent is provided as a term of the employment agreement. This makes confiscation much easier and reduces the chances of a loss of evidence while waiting for legal permission to seize it. Make sure your security policy addresses this important topic.

You should consider the following sources of data when determining what evidence to gather:

- Computer systems involved in the incident (both servers and workstations)
- Logs from security systems (such as intrusion detection, file integrity monitoring, and firewalls)
- Logs from network devices
- Physical access logs
- Other relevant sources of information specific to the incident under investigation

Analysis and Reporting

Once you finish gathering evidence, you should analyze it to determine the most likely course of events leading up to your incident. Summarize those findings in a written report to management. In your report, you should be careful to delineate fact from opinion. It is acceptable to theorize about possible causes, but you should be certain to state which of your conclusions are based entirely on fact and which involve a degree of estimation.

Step 3: Recovery and Remediation

After completing your investigation, you have two tasks remaining: restoring your environment to its normal operating state and completing a “lessons learned” process to improve how you handle future incidents.

Restoration

The goal of the restoration process is to remediate any damage that may have occurred to the organization and limit the damage incurred by similar incidents in the future. These are some of the key actions you should take during this phase:

- Rebuild compromised systems, taking care to remediate any security vulnerabilities that may have contributed to the incident.
- Restore backup data, if necessary, to replace data of questionable integrity.
- Supplement existing security controls, if necessary, to fill gaps identified during the incident analysis.

Once you have completed the restoration process, your business should be back up and running in the state it was in prior to the incident (although in a more secure manner!).

Lessons Learned

The final stage of the incident response process is to conduct a “lessons learned” session. During this important process, members of the incident response team review their actions during the incident and look for potential areas of improvement, both in their actions and in the incident response process. This hindsight review provides an important perspective on the success of your incident response process by analyzing its effectiveness during a real-world incident.

Interviewing Individuals

During your incident investigation, you may find it necessary to speak with individuals who might have information relevant to your investigation. If you seek only to gather information to assist with your investigation, this is called an *interview*. If you suspect the person of involvement in a crime and intend to use the information gathered in court, this is called an *interrogation*.

Interviewing and interrogating individuals are specialized skills and should be performed only by trained investigators. Improper techniques may jeopardize the ability of law enforcement to successfully prosecute an offender. Additionally, many laws govern holding or detaining individuals, and you must abide by them if you plan to conduct private interrogations. Always consult an attorney before conducting any interviews.

Incident Data Integrity and Retention

No matter how persuasive evidence may be, it can be thrown out of court if you somehow alter it during the evidence collection process. Make sure you can prove that you maintained the integrity of all evidence. (Chapter 17 includes more information on evidence rules.) But what about the integrity of data before it is collected?

You may not detect all incidents as they are happening. Sometimes an investigation reveals that there were previous incidents that went undetected. It is discouraging to follow a trail of evidence and find that a key log file that could point back to an attacker has been purged. Carefully consider the fate of log files or other possible evidence locations. A simple archiving policy can help ensure that key evidence is available upon demand no matter how long ago the incident occurred.

Because many log files can contain valuable evidence, attackers often attempt to sanitize them after a successful attack. Take steps to protect the integrity of log files and to deter their modification. One technique is to implement remote logging, where all systems on the network send their log records to a centralized log server that is locked down against attack and does not allow for the modification of data. This technique provides protection from post-incident log file cleansing. Administrators also often use digital signatures to prove that log files were not tampered with after initial capture. For more on digital signatures, see Chapter 10, “PKI and Cryptographic Applications.”

Another important forensic technique is to preserve the original evidence. Remember that the very conduct of your investigation may alter the evidence you are evaluating. Therefore, it’s always best to work with a copy of the actual evidence whenever possible. For example, when conducting an investigation into the contents of a hard drive, make an image of that drive, seal the original drive in an evidence bag, and then use the disk image for your investigation.

As with every aspect of security planning, there is no single solution. Get familiar with your system, and take the steps that make the most sense for your organization to protect it.

Reporting Incidents

When should you report an incident? To whom should you report it? These questions are often difficult to answer. Your security policy should contain guidelines on answering both questions. There is a fundamental problem with reporting incidents. If you report every incident, you run the very real risk of being viewed as a noisemaker. When you have a serious incident, you may be ignored. Also, reporting an unimportant incident could give the impression that your organization is more vulnerable than is the case. This can have a serious detrimental effect on organizations that must maintain strict security. For example, daily incidents at your bank would probably not instill additional confidence in their security practices.

On the other hand, escalation and legal action become more difficult if you do not report an incident soon after discovery. If you delay notifying authorities of a serious incident, you will probably have to answer questions about your motivation for delaying. Even an innocent person could look as if they were trying to hide something by not reporting an incident in a timely manner.

As with most security topics, the answer is not an easy one. In fact, you are compelled by law or regulation to report some incidents. Make sure you know what incidents you must report. For example, any organization that stores credit card information must report any incident in which the disclosure of such information occurred.

Before you encounter an incident, it is wise to establish a relationship with your corporate legal personnel and the appropriate law enforcement agencies. Find out who the appropriate law enforcement contacts are for your organization and talk with them. When the time comes to report an incident, your efforts at establishing a prior working relationship will pay off. You will spend far less time in introductions and explanations if you already know the person with whom you are talking. It is a good idea to identify, in advance, a single point of contact in the organization that will act as your liaison with law enforcement. This provides two benefits. First, it ensures that law enforcement hears a single perspective from your organization and knows the "go-to" person for updates. Second, it allows the predesignated contact to develop working relationships with law enforcement personnel.

TIP

One great way to establish technical contacts with law enforcement is to participate in the FBI's InfraGard program. InfraGard exists in most major metropolitan areas in the United States and provides a forum for law enforcement and business security professionals to share information in a closed environment. For more information, visit www.infragard.net.

Once you determine that you should report an incident, make sure you have as much of the following information as possible:

- What is the nature of the incident, how was it initiated, and by whom?
- When did the incident occur? (Be as precise as possible with dates and times.)
- Where did the incident occur?
- If known, what tools did the attacker use?
- What was the damage resulting from the incident?

You may be asked to provide additional information. Be prepared to provide it in as timely a manner as possible. You may also be asked to quarantine your system.

As with any security action you take, keep a log of all communication, and make copies of any documents you provide as you report an incident.

For more information on incident handling, read NIST SP 800-61, Computer Security Incident Handling Guide, available at http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf, and the Handbook for CSIRTs at www.cert.org/archive/pdf/csirt-handbook.pdf.

Ethics

Security professionals hold themselves and each other to a high standard of conduct because of the sensitive positions of trust they occupy. The rules that govern personal conduct are collectively known as rules of *ethics*. Several organizations have recognized the need for standard ethics rules, or codes, and have devised guidelines for ethical behavior.

We present two codes of ethics in the following sections. These rules are not laws. They are minimum standards for professional behavior. They should provide you with a basis for sound, ethical judgment. As a profession, we expect all security professionals to abide by these guidelines regardless of their area of specialty or employer. Make sure you understand and agree with the codes of ethics outlined in the following sections.

(ISC)² Code of Ethics

The governing body that administers the CISSP certification is the International Information Systems Security Certification Consortium (ISC)². The (ISC)² Code of Ethics was developed to provide the basis for CISSP behavior. It is a simple code with a preamble and four canons. The following is a short summary of the major concepts of the Code of Ethics.

All CISSP candidates should be familiar with the entire (ISC)² Code of Ethics because they have to sign an agreement that they will adhere to this code. We won't cover the code in depth, but you can find further details about the (ISC)²'s Code of Ethics at www.isc2.org/ethics. You need to visit this site and read the entire code.

Code of Ethics Preamble

The Code of Ethics preamble is as follows:

- Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this code is a condition of certification.

Code of Ethics Canons

The Code of Ethics includes the following canons:

Protect society, the commonwealth, and the infrastructure. Security professionals have great social responsibility. We are charged with the burden of ensuring that our actions benefit the common good.

Act honorably, honestly, justly, responsibly, and legally. Integrity is essential to the conduct of our duties. We cannot carry out our duties effectively if others within our organization, the security community, or the general public have doubts about the accuracy of the guidance we provide or the motives behind our actions.

Provide diligent and competent service to principals. Although we have responsibilities to society as a whole, we also have specific responsibilities to those who have hired us to protect their infrastructure. We must ensure that we are in a position to provide unbiased, competent service to our organization.

Advance and protect the profession. Our chosen profession changes on a continuous basis. As security professionals, we must ensure that our knowledge remains current and that we contribute our own knowledge to the community's common body of knowledge.

Ethics and the Internet

In January 1989, the Internet Advisory Board (IAB) recognized that the Internet was rapidly expanding beyond the initial trusted community that created it. Understanding that misuse could occur as the Internet grew, IAB issued a statement of policy concerning the proper use of the Internet. The contents of this statement are valid even today. It is important that you know the basic contents of the document, titled "Ethics and the Internet," Request for Comments (RFC) 1087, because most codes of ethics can trace their roots back to this document.

The statement is a brief list of practices considered unethical. Where a code of ethics states what you should do, this document outlines what you should not do. RFC 1087 states that any activity with the following purposes is unacceptable and unethical:

- Seeks to gain unauthorized access to the resources of the Internet
- Disrupts the intended use of the Internet
- Wastes resources (people, capacity, computer) through such actions
- Destroys the integrity of computer-based information
- Compromises the privacy of users

Ten Commandments of Computer Ethics

The Computer Ethics Institute created its own code of ethics. The Ten Commandments of Computer Ethics are as follows:

1. Thou shalt not use a computer to harm other people.

2. Thou shalt not interfere with other people's computer work.

3. Thou shalt not snoop around in other people's computer files.

4. Thou shalt not use a computer to steal.

5. Thou shalt not use a computer to bear false witness.

6. Thou shalt not copy proprietary software for which you have not paid.

7. Thou shalt not use other people's computer resources without authorization or proper compensation.

8. Thou shalt not appropriate other people's intellectual output.

9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.

10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

There are many ethical and moral codes of IT behavior to choose from. Another system you should consider is the Generally Accepted Systems Security Principles (GASSP). You can find the full text of the GASSP system at www.infosectoday.com/Articles/gassp.pdf.

Summary

Computer crimes are grouped into several major categories, and the crimes in each category share common motivations and desired results. Understanding what an attacker is after can help in properly securing a system.

For example, military and intelligence attacks are launched to acquire secret information that could not be obtained legally. Business attacks are similar except that they target civilian systems. Other types of attacks include financial attacks (phone phreaking is an example of a financial attack) and terrorist attacks (which, in the context of computer crimes, are attacks designed to disrupt normal life). Finally, there are grudge attacks, the purpose of which is to cause damage by destroying data or using information to embarrass an organization or person, and thrill attacks, launched by inexperienced crackers to compromise or disable a system. Although generally not sophisticated, thrill attacks can be annoying and costly.

An incident is a violation or the threat of a violation of your security policy. When an incident is suspected, you should immediately begin an investigation and collect as much evidence as possible because, if you decide to report the incident, you must have enough admissible evidence to support your claims.

The set of rules that govern your personal behavior is a code of ethics. There are several codes of ethics, from general to specific in nature, which security professionals can use to guide them. The (ISC)² makes the acceptance of its code of ethics a requirement for certification.

Exam Essentials

Know the definition of computer crime. Computer crime is a crime (or violation of a law or regulation) that is directed against, or directly involves, a computer.

Be able to list and explain the six categories of computer crimes. Computer crimes are grouped into six categories: military and intelligence attack, business attack, financial attack, terrorist attack, grudge attack, and thrill attack. Be able to explain the motive of each type of attack.

Know the importance of collecting evidence. As soon you discover an incident, you must begin to collect evidence and as much information about the incident as possible. The evidence can be used in a subsequent legal action or in finding the identity of the attacker. Evidence can also assist you in determining the extent of damage.

Understand that an incident is any violation, or threat of a violation, of your security policy. Incidents should be defined in your security policy. Even though specific incidents may not be outlined, the existence of the policy sets the standard for the use of your system. An incident is any event that has a negative outcome affecting the confidentiality, integrity, or availability of an organization's data.

Be able to list the four common types of incidents, and know the telltale signs of each. An incident occurs when an attack or other violation of your security policy is carried out against your system. Incidents can be grouped into four categories: scanning, compromises, malicious code, and denial of service. Be able to explain what each type of incident involves and what signs to look for.

Know the importance of identifying abnormal and suspicious activity. Attacks will generate some activity that is not normal. Recognizing abnormal and suspicious activity is the first step toward detecting incidents.

Know how to investigate intrusions and how to gather sufficient information from the equipment, software, and data. You must have possession of equipment, software, or data to analyze it and use it as evidence. You must acquire the evidence without modifying it or allowing anyone else to modify it.

Know the three basic alternatives for confiscating evidence and when each one is appropriate. First, the person who owns the evidence could voluntarily surrender it. Second, a subpoena could be used to compel the subject to surrender the evidence. Third, a search warrant is most useful when you need to confiscate evidence without giving the subject an opportunity to alter it.

Know the importance of retaining incident data. Because you will discover some incidents after they have occurred, you will lose valuable evidence unless you ensure that critical log files are retained for a reasonable period of time. You can retain log files and system status information either in place or in archives.

Be familiar with how to report an incident. The first step is to establish a working relationship with the corporate and law enforcement personnel with whom you will work to resolve an incident. When you do have a need to report an incident, gather as much descriptive information as possible and make your report in a timely manner.

Understand the importance of ethics to security personnel. Security practitioners are granted a very high level of authority and responsibility to execute their job functions. The potential for abuse exists, and without a strict code of personal behavior, security practitioners could be regarded as having unchecked power. Adherence to a code of ethics helps ensure that such power is not abused.

Know the (ISC)^2 Code of Ethics and RFC 1087, "Ethics and the Internet." All CISSP candidates should be familiar with the entire (ISC)^2 Code of Ethics because they have to sign an agreement that they will adhere to it. In addition, be familiar with the basic statements of RFC 1087.

Written Lab

1. What are the major categories of computer crime?

2. What is the main motivation behind a thrill attack?

3. What is the difference between an interview and an interrogation?

4. What is the difference between an event and an incident?

5. Who are the common members of an incident response team?

6. What are the three phases of the incident response process?

Answers to Written Lab

1. The major categories of computer crime are military/intelligence attacks, business attacks, financial attacks, terrorist attacks, grudge attacks, and thrill attacks.

2. Thrill attacks are motivated by individuals seeking to achieve the "high" associated with successfully breaking into a computer system.

3. Interviews are conducted with the intention of gathering information to assist with your investigation. Interrogations are conducted with the intent of gathering evidence to be used in a criminal prosecution.

4. An event is any occurrence that takes place during a certain period of time. Incidents are events that have negative outcomes affecting the confidentiality, integrity, or availability of your data.

5. Incident response teams normally include representatives from senior management, information security professionals, legal representatives, public affairs/communications representatives, and technical engineers.

6. The three phases of the incident response process are detection and identification, response and reporting, and recovery and remediation.

Review Questions

1. What is a computer crime?

A. Any attack specifically listed in your security policy

B. Any illegal attack that compromises a protected computer

C. Any violation of a law or regulation that involves a computer

D. Failure to practice due diligence in computer security

2. What is the main purpose of a military and intelligence attack?

A. To attack the availability of military systems

B. To obtain secret and restricted information from military or law enforcement sources

C. To utilize military or intelligence agency systems to attack other nonmilitary sites

D. To compromise military systems for use in attacks against other systems

3. What type of attack targets proprietary information stored on a civilian organization's system?

A. Business attack

B. Denial-of-service attack

C. Financial attack

D. Military and intelligence attack

4. What goal is not a purpose of a financial attack?

A. Access services you have not purchased.

B. Disclose confidential personal employee information.

C. Transfer funds from an unapproved source into your account.

D. Steal money from another organization.

5. Which one of the following attacks is most indicative of a terrorist attack?

A. Alter sensitive trade secret documents.

B. Damage the ability to communicate and respond to a physical attack.

C. Steal unclassified information.

D. Transfer funds to other countries.

6. Which of the following would not be a primary goal of a grudge attack?

A. Disclose embarrassing personal information.

B. Launch a virus on an organization's system.

C. Send inappropriate email with a spoofed origination address of the victim organization.

D. Use automated tools to scan the organization's systems for vulnerable ports.

7. What are the primary reasons attackers engage in thrill attacks? (Choose all that apply.)

A. Bragging rights

B. Money from the sale of stolen documents

C. Pride of conquering a secure system

D. Retaliation against a person or organization

8. What is the most important rule to follow when collecting evidence?

A. Do not turn off a computer until you photograph the screen.

B. List all people present while collecting evidence.

C. Never modify evidence during the collection process.

D. Transfer all equipment to a secure storage location.

9. What would be a valid argument for not immediately removing power from a machine when an incident is discovered?

A. All of the damage has been done. Turning the machine off would not stop additional damage.

B. There is no other system that can replace this one if it is turned off.

C. Too many users are logged in and using the system.

D. Valuable evidence in memory will be lost.

10. What is the reason many incidents are never reported?

A. It involves too much paperwork.

B. Reporting too many incidents could hurt an organization's reputation.

C. The incident is never discovered.

D. Too much time has passed, and the evidence is gone.

11. What is an incident?

A. Any active attack that causes damage to your system

B. Any violation of a code of ethics

C. Any crime (or violation of a law or regulation) that involves a computer

D. Any event that adversely affects the confidentiality, integrity or availability of your data

12. If port scanning does no damage to a system, why is it generally considered an incident?

A. All port scans indicate adversarial behavior.

B. Port scans can precede attacks that cause damage and can indicate a future attack.

C. Scanning a port damages the port.

D. Port scanning uses system resources that could be put to better uses.

13. What type of incident is characterized by obtaining an increased level of privilege?

A. Compromise

B. Denial of service

C. Malicious code

D. Scanning

14. What is the best way to recognize abnormal and suspicious behavior on your system?

A. Be aware of the newest attacks.

B. Configure your IDS to detect and report all abnormal traffic.

C. Know what your normal system activity looks like.

D. Study the activity signatures of the main types of attacks.

15. If you need to confiscate a PC from a suspected attacker who does not work for your organization, what legal avenue is most appropriate?

A. Consent agreement signed by employees

B. Search warrant

C. No legal avenue is necessary

D. Voluntary consent

16. Why should you avoid deleting log files on a daily basis?

A. An incident may not be discovered for several days and valuable evidence could be lost.

B. Disk space is cheap, and log files are used frequently.

C. Log files are protected and cannot be altered.

D. Any information in a log file is useless after it is several hours old.

17. Which of the following conditions might require that you report an incident? (Choose all that apply.)

A. Confidential information protected by government regulation was possibly disclosed.

B. Damages exceeded $1,500.

C. The incident has occurred before.

D. The incident resulted in a violation of a law.

18. What are ethics?

A. Mandatory actions required to fulfill job requirements

B. Laws of professional conduct

C. Regulations set forth by a professional organization

D. Rules of personal behavior

19. According to the (ISC)^2 Code of Ethics, how are CISSPs expected to act?

A. Honestly, diligently, responsibly, and legally

B. Honorably, honestly, justly, responsibly, and legally

C. Upholding the security policy and protecting the organization

D. Trustworthy, loyally, friendly, courteously

20. Which of the following actions are considered unacceptable and unethical according to RFC 1087, “Ethics and the Internet”?

A. Actions that compromise the privacy of classified information

B. Actions that compromise the privacy of users

C. Actions that disrupt organizational activities

D. Actions in which a computer is used in a manner inconsistent with a stated security policy

Answers to Review Questions

1. C. A crime is any violation of a law or regulation. The violation stipulation defines the action as a crime. It is a computer crime if the violation involves a computer either as the target or as a tool.

2. B. A military and intelligence attack is targeted at the classified data that resides on the system. To the attacker, the value of the information justifies the risk associated with such an attack. The information extracted from this type of attack is often used to plan subsequent attacks.

3. A. Confidential information that is not related to the military or intelligence agencies is the target of business attacks. The ultimate goal could be destruction, alteration, or disclosure of confidential information.

4. B. A financial attack focuses primarily on obtaining services and funds illegally.

5. B. A terrorist attack is launched to interfere with a way of life by creating an atmosphere of fear. A computer terrorist attack can reach this goal by reducing the ability to respond to a simultaneous physical attack.

6. D. Any action that can harm a person or organization, either directly or through embarrassment, would be a valid goal of a grudge attack. The purpose of such an attack is to “get back” at someone.

7. A, C. Thrill attacks have no reward other than providing a boost to pride and ego. The thrill of launching the attack comes from the act of participating in the attack (and not getting caught).

8. C. Although the other options have some merit in individual cases, the most important rule is to never modify, or taint, evidence. If you modify evidence, it becomes inadmissible in court.

9. D. The most compelling reason for not removing power from a machine is that you will lose the contents of memory. Carefully consider the pros and cons of removing power. After all is considered, it may be the best choice.

10. C. Although an organization would not want to report a large number of incidents (unless reporting them is mandatory), the reality is that many incidents are never discovered. The lack of well-trained users results in many incidents that are never recognized.

11. D. An incident is normally defined as any event that adversely affects the confidentiality, integrity, or availability of your data.

12. B. Some port scans are normal. An unusually high volume of port scan activity can be a reconnaissance activity preceding a more dangerous attack. When you see unusual port scanning, you should always investigate.

13. A. Any time an attacker exceeds their authority, the incident is classified as a system compromise. This includes valid users who exceed their authority as well as invalid users who gain access through the use of a valid user ID.

14. C. Although options A, B, and D are actions that can make you aware of what attacks look like and how to detect them, you will never successfully detect most attacks until you know your system. When you know what the activity on your system looks like on a normal day, you can immediately detect any abnormal activity.

15. B. In this case, you need a search warrant to confiscate equipment without giving the suspect time to destroy evidence. If the suspect worked for your organization and you had all employees sign consent agreements, you could simply confiscate the equipment.

16. A. Log files contain a large volume of generally useless information. However, when you are trying to track down a problem or an incident, they can be invaluable. Even if an incident is discovered as it is happening, it may have been preceded by other incidents. Log files provide valuable clues and should be protected and archived.

17. A, D. You must report an incident when the incident resulted in the violation of a law or regulation. This includes any damage (or potential damage) to or disclosure of protected information.

18. D. Ethics are simply rules of personal behavior. Many professional organizations establish formal codes of ethics to govern their members, but ethics are personal rules individuals use to guide their lives.

19. B. The second canon of the (ISC)² Code of Ethics states how a CISSP should act, which is honorably, honestly, justly, responsibly, and legally.

20. B. RFC 1087 does not specifically address the statements in A, C, or D. Although each type of activity listed is unacceptable, only the activity identified in option B is identified in RFC 1087.

Chapter 19

Physical Security Requirements

THE CISSP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

- **Operations Security**
    - Manage incident response
        - Detection; response; reporting; recovery; remediation
- **Physical (Environmental) Security**
    - Participate in site and facility design considerations
    - Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)

    - Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)
    - Support the implementation and operation of facilities security
        - Communications and server rooms; restricted and work area security; data center security; utilities and HVAC considerations; water issues (e.g., leakage, flooding); fire prevention, detection and suppression
    - Support the protection and securing of equipment

Among numerous other topics, the Operations Security domain of the Common Body of Knowledge (CBK) for the CISSP certification exam deals with managing incident response as and when a security indicent occurs. It also delves into the mechanics of such a response, including detecting that an incident has occurred, and then responding to, reporting on, and recovering from or remediating its results.

The Physical (Environmental) Security domain of the Common Body of Knowledge (CBK) for the CISSP certification exam deals with topics and issues related to facility construction and location, the security features of a facility, forms of physical access control, types of physical security technical controls, and maintaining security by properly sustaining the environment and protecting human life.

The purpose of physical security is to protect against physical threats. The following physical threats are among the most common:

- Fire and smoke
- Water (rising/falling)
- Earth movement (earthquakes, landslides, volcanoes)
- Storms (wind, lightning, rain, snow, sleet, ice)
- Sabotage/vandalism
- Explosion/destruction
- Building collapse
- Toxic materials
- Utility loss (power, heating, cooling, air, water)
- Equipment failure
- Personnel loss (strikes, illness, access, transport)

This chapter explores each of these issues and discusses safeguards and countermeasures to protect against them. In many cases, you'll need a disaster recovery plan or a business continuity plan should a serious physical threat (such as an explosion, sabotage, or natural disaster) occur. Chapters 15, "Business Continuity Planning," and 16, "Disaster Recovery Planning," cover those topics in detail.

Facility Requirements

It should be blatantly obvious if you've read the previous 18 chapters that without control over the physical environment, no collection of administrative, technical, or logical access controls can provide adequate security. If a malicious person can gain physical access to your facility or equipment, they can do just about anything they want, from destruction to disclosure or alteration. Physical controls are your first line of defense, and people are your last.

There are many aspects of and elements to implementing and maintaining physical security. A core or foundational element is selecting or designing the facility to house your IT infrastructure and your organization's operations. The process of selecting or designing a secure facility always starts with a plan.

Secure Facility Plan

A secure facility plan outlines the security needs of your organization and emphasizes methods or mechanisms to employ to provide security. Such a plan is developed through a process known as *critical path analysis*. Critical path analysis is a systematic effort to identify relationships between mission-critical applications, processes, and operations and all the necessary supporting elements. For example, an e-commerce server used to sell products over the Web relies on Internet access, computer hardware, electricity, temperature control, storage facility, and so on.

When critical path analysis is performed properly, a complete picture of the interdependencies and interactions necessary to sustain the organization is produced. Once that analysis is complete, its results serve as a list of items to secure. The first step in designing a secure IT infrastructure is providing security for the basic requirements of the organization and its computers. These basic requirements include electricity, environmental controls (in other words, a building, air conditioning, heating, humidity control, and so on), and water/sewage.

Security staff should participate in site and facility design considerations. Otherwise, many important aspects of physical security essential for the existence of logical security may be overlooked. With security staff involved in the physical facility design, you can be assured that your long-term security goals as an organization will be supported not just by your policies, personnel, and electronic equipment, but by the building itself.

Physical Security Controls

The security controls implemented to manage physical security can be divided into three groups: administrative, technical, and physical. Because these are the same categories used to describe access controls, it is vital to focus on the physical security aspects of these controls. *Administrative physical security controls* include facility construction and selection, site management, personnel controls, awareness training, and emergency response and procedures. *Technical physical security controls*include access controls; intrusion detection; alarms; closed-circuit television (CCTV); monitoring; heating, ventilating, and air conditioning (HVAC); power supplies; and fire detection and suppression. *Physical controls for physical security* include fencing, lighting, locks, construction materials, mantraps, dogs, and guards.

Corporate vs. Personal Property

Physical security controls embrace both visible and invisible aspects in many ordinary business environments. You see them at the post office, at the corner store, and in certain areas of your own computing environment. They are so pervasive that some people choose where they live based on their presence, as in gated access communities or secure apartment complexes.

Alison is a security analyst for a major technology corporation that specializes in data management. This company includes an in-house security staff (guards, administrators, and so on) that is capable of handling physical security breaches.

Brad experienced an intrusion—into his personal vehicle in the company parking lot. He asks Alison whether she observed or recorded anyone breaking into and entering his vehicle, but this is a personal item and not a company possession, and she has no control or regulation over damage to employee assets.

This is understandably unnerving for Brad, but he understands that she's protecting the business and not his belongings. When or where would you think it would be necessary to implement security measures for both? The usual answer is anywhere business assets are or might be involved. Had Brad been using a company vehicle parked in the company parking lot, then perhaps Alison could make allowances for an incidental break-in involving Brad's things, but even then she isn't responsible for their safekeeping. On the other hand, where key people are also important assets (executive staff at most enterprises, security analysts who work in sensitive positions, heads of state, and so forth), protection and safeguards usually extend to embrace them and their belongings as part of asset protection and risk mitigation. Of course, if danger to employees or what they carry with them becomes a problem, securing the parking garage with key cards and installing CCTV monitors on every floor really begins to make sense. Simply put, if the costs of allowing break-ins to occur exceeds that of installing preventive measures, it's prudent to put them in place.

When designing physical security for an environment, focus on the functional order of controls. Security controls should be deployed so that initial attempts to access physical assets are deterred (in other words, boundary restrictions). If deterrence fails, then direct access to physical assets should be denied (for example, locked vault doors). If denial fails, your system needs to detect intrusion (for example, using motion detectors), and the intrusion should be delayed sufficiently to enable authorities to respond (for example, a cable lock on the asset). It's important to remember this order when deploying physical security controls: first deterrence, then denial, then detection, then delay.

Site Selection

Site selection should be based on the security needs of the organization. Cost, location, and size are important, but addressing the requirements of security should always take precedence. When choosing a site on which to build a facility or selecting a preexisting structure, be sure to examine every aspect of its location carefully.

Securing assets depends largely on site security, which involves numerous considerations and situational elements. Site location and construction play a crucial role in the overall site selection process. Susceptibility to riots, looting, break-ins, and vandalism or location within a high-crime area are obviously all poor choices but cannot always be dictated or controlled. Environmental threats such as fault lines, tornado/hurricane regions, and close proximity to other natural disasters present significant issues for the site selection process as well because you can’t always avoid such threats.

Proximity to other buildings and businesses is another crucial consideration. What sorts of attention do they draw, and how does that affect your operation or facility? Proximity to emergency-response personnel is another consideration, along with other elements. Some companies can afford to buy or build their own campuses to keep neighboring elements out of play and to enable tighter access control and monitoring. However, not every company can exercise this option and must make do with what’s available and affordable instead.

At a minimum, ensure that the building is designed to withstand fairly extreme weather conditions and that it can deter or fend off overt break-in attempts. Vulnerable entry points such as windows and doors tend to dominate such analysis, but you should also evaluate objects (trees, shrubs, or man-made items) that can obscure break-in attempts.

Visibility

Visibility is important. What is the surrounding terrain? Would it be easy to approach the facility by vehicle or on foot without being seen? The makeup of the surrounding area is also important. Is it in or near a residential, business, or industrial area? What is the local crime rate? Where are the closest emergency services located (fire, medical, police)? What unique hazards may be found in the vicinity (chemical plants, homeless shelters, universities, construction sites, and so on)?

Accessibility and Perimeter Security

The accessibility to the building or campus location is also important. Single entrances are great for providing security, but multiple entrances are better for evacuation during emergencies. What types of roads are nearby? What means of transportation are easily accessible (trains, highway, airport, shipping)? What about traffic levels throughout the day?

Keep in mind that accessibility is also constrained by the need for perimeter security. The needs of access and use should meld and support the implementation and operation of perimeter security. The use of physical access controls and monitoring personnel and equipment entering and leaving as well as auditing/logging all physical events are key elements in maintaining overall organizational security.

Natural Disasters

Another concern is the potential impact that natural disasters could make in the area. Is it prone to earthquakes, mudslides, sinkholes, fires, floods, hurricanes, tornadoes, falling rocks, snow, rainfall, ice, humidity, heat, extreme cold, and so on? You must prepare for natural disasters and equip your IT environment to either survive an event or be replaced easily.

Facility Design

When designing the construction of a facility, you must understand the level of security that your organization needs. A proper level of security must be planned and designed before construction begins.

Important issues to consider include combustibility, fire rating, construction materials, load rating, placement, and control of items such as walls, doors, ceilings, flooring, HVAC, power, water, sewage, gas, and so on. Forced intrusion, emergency access, resistance to entry, direction of entries and exits, use of alarms, and conductivity are other important aspects to evaluate. Every element within a facility should be evaluated in terms of how it could be used for and against the protection of the IT infrastructure and personnel (for example, positive flows for air and water from inside a facility to outside its boundaries).

There's also a pretty well-established school of thought on "secure architecture" that's often called crime prevention through environmental design (CPTED). The guiding idea is to structure the physical environment and surroundings to influence individual decisions that potential offenders make before committing any criminal acts. The International CPTED Association is an excellent source for information on this subject (www.cpted.net), as is Oscar Newman's book *Creating Defensible Space*, published by HUD's Office of Policy Development and Research (free PDF download at www.defensiblespace.com/book.htm).

Work Areas

The design and configuration of work areas and visitor areas should be considered carefully. There should not be equal access to all locations within a facility. Areas that contain assets of higher value or importance should have more restricted access. For example, anyone who enters the facility should be able to access the restrooms and the public telephone without going into sensitive areas, but only network administrators and security staff should have access to the server room. Valuable and confidential assets should be located in the heart or center of protection provided by a facility. In effect, you should focus on deploying concentric circles of physical protection. This type of configuration requires increased levels of authorization to gain access into more sensitive areas inside the facility.

Walls or partitions can be used to separate similar but distinct work areas. Such divisions deter casual shoulder surfing or eavesdropping (*shoulder surfing* is the act of gathering information from a system by observing the monitor or the use of the keyboard by the operator). Floor-to-ceiling walls should be used to separate areas with differing levels of sensitivity and confidentiality (where false or suspended ceilings are present, walls should cut these off as well to provide an unbroken physical barrier between more and less secure areas).

Each work area should be evaluated and assigned a classification just as IT assets are classified. Only people with clearance or classifications corresponding to the classification of the work area should be allowed access. Areas with different purposes or uses should be assigned different levels of access or restrictions. The more access to assets the equipment within an area offers, the more important become the restrictions that are used to control who enters those areas and what activities they are allowed to perform.

Your facility security design process should support the implementation and operation of internal security. In addition to the management of workers in proper work spaces, you should address visitors. Should there be an escort requirement for visitors, and what other forms of visitor control should be implemented? In addition to basic physical security tools such as keys and locks, mechanisms such as mantraps, video cameras, written logs, security guards, and RFID ID tags should be implemented.

Server Rooms

Server rooms, server vaults, and IT closets are enclosed, restricted, and protected rooms where your mission-critical servers and network devices are housed. Centralized server rooms need not be human compatible. In fact, the more human incompatible a server room is, the more protection it will offer against casual and determined attacks. Human incompatibility can be accomplished by including Halotron, PyroGen, or other halon-substitute oxygen-displacement fire detection and extinguishing systems, low temperatures, little or no lighting, and equipment stacked with little room to maneuver. Server rooms should be designed to support optimal operation of the IT infrastructure and to block unauthorized human access or intervention.

Server rooms should be located at the core of the building. Try to avoid locating these rooms on the ground floor, the top floor, and the basement whenever possible. Additionally, the server room should be located away from water, gas, and sewage lines. These pose too large a risk of leakage or flooding, which can cause serious damage and downtime.

The walls of your server room should also have a one-hour minimum fire rating.

Real World Scenario

Making Servers Inaccessible

The running joke in the IT security realm is that the most secure computer is one that is disconnected from the network and sealed in a room with no doors or windows. No, seriously, that’s the joke. But there’s a massive grain of truth and irony in it as well.

Carlos operates security processes and platforms for a financial banking firm, and he knows all about one-way systems and unreachable devices. Sensitive business transactions occur in fractions of a second, and one wrong move could pose serious risks to data and involved parties.

In his experience, Carlos knows that the least accessible and least human-friendly places are his most valuable assets, so he stores many of his machines inside a separate bank vault. You’d have to be a talented burglar, a skilled safecracker, and a determined computer attacker to breach his security defenses.

Not all business applications and processes warrant this extreme sort of prevention. What security recommendations might you suggest to make a server more inconvenient or inaccessible, short of dedicating a vault? A basement with limited access or an interior room with no windows and only one entry/exit point makes an excellent substitute when an empty vault isn’t available. The key is to select a space with limited access and then to establish serious hurdles to entry (especially unauthorized entry). CCTV monitoring on the door and motion detectors inside the space can also help maintain proper attention to who is coming and going.

Visitors

If a facility employs restricted areas to control physical security, a mechanism to handle visitors is required. Often an escort is assigned to visitors, and their access and activities are monitored closely. Failing to track the actions of outsiders when they are allowed into a protected area can result in malicious activity against the most protected assets.

Real World Scenario

Deploying Physical Access Controls

In the real world, you will deploy multiple layers of physical access controls to manage the traffic of authorized and unauthorized individuals within your facility. The outermost layer will be lighting. The entire outer perimeter of your site should be clearly lit. This enables easy identification of personnel and makes it easier to notice intrusions and intimidate potential intruders. Just inside the lighted area, place a fence or wall designed to prevent intrusion. Specific controlled points along that fence or wall should be points for entry or exit. These should have gates, turnstiles, or mantraps all monitored by CCTV and security guards. Identification and authentication should be required at all entry points before entrance is granted.

Within the facility, areas of different sensitivity or confidentiality levels should be distinctly separated and compartmentalized. This is especially true for public areas and areas accessible to visitors. An additional identification/authentication process to validate the need to enter should be required when anyone moves from one area to another. The most sensitive resources and systems should be isolated from all but the most privileged personnel and located at the center or core of the facility.

Forms of Physical Access Controls

You can deploy many types of physical access control mechanisms in an environment to control, monitor, and manage access to a facility. These range from deterrents to detection mechanisms.

The various sections, divisions, or areas within a site or facility should be clearly designated as public, private, or restricted. Each of these areas requires unique and focused physical access controls, monitoring, and prevention mechanisms. The following sections discuss many such mechanisms that may be used to separate, isolate, and control access to various areas within a site.

Fences, Gates, Turnstiles, and Mantraps

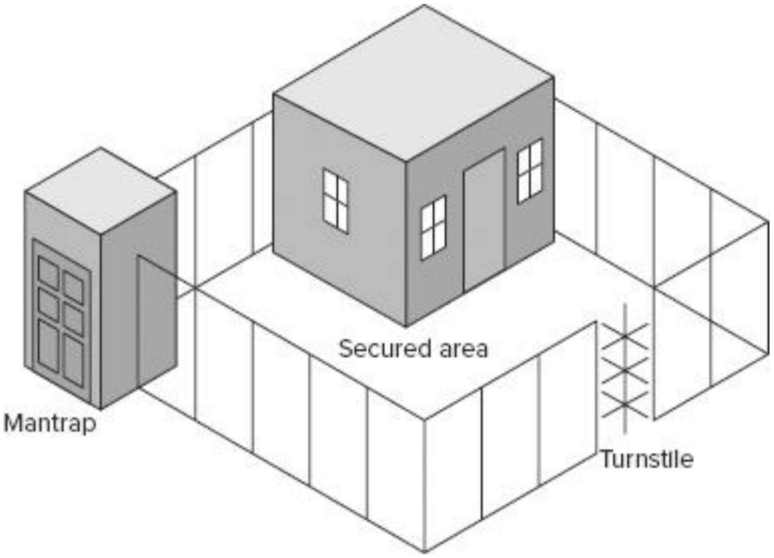
A *fence* is a perimeter-defining device. Fences are used to clearly differentiate between areas that are under a specific level of security protection and those that aren't. Fencing can include a wide range of components, materials, and construction methods. It can consist of stripes painted on the ground, chain link fences, barbed wire, concrete walls, and even invisible perimeters using laser, motion, or heat detectors. Various types of fences are effective against different types of intruders:

- Fences 3 to 4 feet high deter casual trespassers.
- Fences 6 to 7 feet high are too hard to climb easily and deter most intruders, except determined ones.
- Fences 8 or more feet high with three strands of barbed wire deter even determined intruders.

A *gate* is a controlled exit and entry point in a fence. The deterrent level of a gate must be equivalent to the deterrent level of the fence to sustain the effectiveness of the fence as a whole. Hinges and locking/closing mechanisms should be hardened against tampering, destruction, or removal. When a gate is closed, it should not offer any additional access vulnerabilities. Keep the number of gates to a minimum. They can be manned by guards or not. When they're not protected by guards, use of dogs or CCTV is recommended.

A *turnstile* (see Figure 19.1) is a form of gate that prevents more than one person at a time from gaining entry and often restricts movement in one direction. It is used to gain entry but not to exit or vice versa. A turnstile is basically the fencing equivalent of a secured revolving door.

FIGURE 19.1 A secure physical boundary with a mantrap and a turnstile



A *mantrap* is a double set of doors that is often protected by a guard (also shown in Figure 19.1) or some other physical layout that prevents piggybacking and can trap individuals at the discretion of security personnel. The purpose of a mantrap is to immobilize a subject until their identity and authentication is verified. If a subject is authorized for entry, the inner door opens, allowing entry into the facility or onto the premises. If a subject is not authorized, both doors remain closed and locked until an escort (typically a guard or a police officer) arrives to escort the subject off the property or arrest the subject for trespassing (this is called a *delay* feature). Often a mantrap includes a scale to prevent piggybacking or tailgating.

Lighting

Lighting is a commonly used form of perimeter security control. The primary purpose of lighting is to discourage casual intruders, trespassers, prowlers, or would-be thieves who would rather perform their misdeeds in the dark. However, lighting is not a strong deterrent. It should not be used as the primary or sole protection mechanism except in areas with a low threat level.

Lighting should not illuminate the positions of guards, dogs, patrol posts, or other similar security elements. It should be combined with guards, dogs, CCTV, or some other form of intrusion detection or surveillance mechanism. Lighting must not cause a nuisance or problem for nearby residents, roads, railways, airports, and so on. It should also never cause glare or reflective distraction to guards, dogs, and monitoring equipment, which could otherwise aid attackers during break-in attempts.

The National Institute of Standards and Technology (NIST) standard for perimeter protection using lighting is that critical areas should be illuminated with 2 candle feet of power at a height of 8 feet. Another common issue for the use of lighting is the placement of the lights. Standards seem to indicate that light poles should be placed the same distance apart as the diameter of the illuminated area created by illumination elements. Thus, if a lighted area is 40 feet in diameter, poles should be 40 feet apart.

Security Guards and Dogs

All physical security controls, whether static deterrents or active detection and surveillance mechanisms, ultimately rely upon personnel to intervene and stop actual intrusions and attacks. Security guards exist to fulfill this need. Guards can be posted around a perimeter or inside to monitor access points or watch detection and surveillance monitors. The real benefit of guards is that they are able to adapt and react to various conditions or situations. Guards can learn and recognize attack and intrusion activities and patterns, can adjust to a changing environment, and can make decisions and judgment calls. Security guards are often an appropriate security control when immediate situation handling and decision making onsite is necessary.

Unfortunately, using security guards is not a perfect solution. There are numerous disadvantages to deploying, maintaining, and relying upon security guards. Not all environments and facilities support security guards. This may be because of actual human incompatibility or the layout, design, location, and construction of the facility. Not all security guards are themselves reliable. Prescreening, bonding, and training do not guarantee that you won't end up with an ineffective or unreliable security guard.

Even if a guard is initially reliable, guards are subject to physical injury and illness, take vacations, can become distracted, are vulnerable to social engineering, and may become unemployable because of substance abuse. In addition, they sometimes focus on self-preservation instead of preserving security at the guarded facility. This may mean that security guards can offer protection only up to the point at which their life is endangered. Additionally, security guards are usually unaware of the scope of the operations within a facility and are therefore not thoroughly equipped to know how to respond to every situation. Finally, security guards are expensive.

Guard dogs can be an alternative to security guards. They can often be deployed as a perimeter security control. As a detection and deterrent, dogs are extremely effective. However, dogs are costly, require a high level of maintenance, and impose serious insurance and liability requirements.

Keys and Combination Locks

Locks keep closed doors closed. They are designed and deployed to prevent access to everyone without proper authorization. A *lock* is a crude form of an identification and authorization mechanism. If you possess the correct key or combination, you are considered authorized and permitted entry. Key-based locks are the most common and inexpensive forms of physical access control devices. These are often known as *preset locks*. These types of locks are subject to picking, which is often categorized under a class of lock mechanism attacks called *shimming*.

Real World Scenario

Using Locks

Keys or combination locks—which do you choose and for what purposes?

Ultimately, there will always be that forgetful element of users who just cannot be reminded enough. Elise constantly forgets her combination, and Francis can never remember to bring his security key card to work. Gino maintains a pessimistic outlook in his administrative style, so he’s keen on putting combinations and key card accesses in all the right places.

Under what circumstances or conditions might you employ a combination lock, and where might you instead opt for a key or key card? What options put you at greater risk of loss if someone discovers the combination or finds the key? Can you be certain that these single points of failure do not significantly pose a risk to the protected assets?

Many organizations typically utilize separate forms of key or combination accesses throughout several areas of the facility. Key and key card access is granted at select shared entry points (exterior access into the building, access into interior rooms), and combination locks control access to individual entry points (storage lockers, file cabinets, and so on).

Programmable or combination locks offer a broader range of control than preset locks. Some programmable locks can be configured with multiple valid access combinations or may include digital or electronic controls employing keypads, smart cards, or cipher devices. For instance, an *electronic access control (EAC)* lock incorporates three elements: an electromagnet to keep the door closed, a credential reader to authenticate subjects and to disable the electromagnet, and a sensor to reengage the electromagnet when the door is closed.

Locks serve as an alternative to security guards as a perimeter entrance access control device. A gate or door can be opened and closed to allow access by a security guard who verifies your identity before granting access, or the lock itself can serve as the verification device that also grants or restricts entry.

Badges

Badges, *identification cards*, and *security IDs* are forms of physical identification and/or electronic access control devices. A badge can be as simple as a name tag indicating whether you are a valid employee or a visitor. Or it can be as complex as a smart card or token device that employs multifactor authentication to verify and prove your identity and provide authentication and authorization to access a facility, specific rooms, or secured workstations. Badges often include pictures, magnetic strips with encoded data, and personal details to help a security guard verify identity.

Badges can be used in environments in which physical access is primarily controlled by security guards. In such conditions, the badge serves as a visual identification tool for the guards. They can verify your identity by comparing your picture to your person and consult a printed or electronic roster of authorized personnel to determine whether you have valid access.

Badges can also serve in environments guarded by scanning devices rather than security guards. In such conditions, a badge can be used either for identification or for authentication. When a badge is used for identification, it is swiped in a device, and then the badge owner must provide one or more authentication factors, such as a password, passphrase, or biological trait (if a biometric device is used). When a badge is used for authentication, the badge owner provides an ID, username, and so on and then swipes the badge to authenticate.

Motion Detectors

A *motion detector*, or *motion sensor*, is a device that senses motion in a specific area. Many types of motion detectors exist, including infrared, heat, wave pattern, capacitance, photoelectric, and passive audio. An infrared motion detector monitors for significant or meaningful changes in the infrared lighting pattern of a monitored area. A heat-based motion detector monitors for significant or meaningful changes in the heat levels and patterns in a monitored area. A wave pattern motion detector transmits a consistent low ultrasonic or high microwave frequency signal into a monitored area and monitors for significant or meaningful changes or disturbances in the reflected pattern. A capacitance motion detector senses changes in the electrical or magnetic field surrounding a monitored object. A photoelectric motion detector senses changes in visible light levels for the monitored area. Photoelectric motion detectors are usually deployed in internal rooms that have no windows and are kept dark. A passive audio motion detector listens for abnormal sounds in the monitored area.

Intrusion Alarms

Whenever a motion detector registers a significant or meaningful change in the environment, it triggers an alarm. An *alarm* is a separate mechanism that triggers a deterrent, a repellent, and/or a notification. Alarms that trigger deterrents may engage additional locks, shut doors, and so on. The goal of such an alarm is to make further intrusion or attack more difficult.

Alarms that trigger repellants usually sound an audio siren or bell and turn on lights. These kinds of alarms are used to discourage intruders or attackers from continuing their malicious or trespassing activities and force them off the premises. Alarms that trigger notification are often silent from the intruder/attacker perspective but record data about the incident and notify administrators, security guards, and law enforcement. A recording of an incident can take the form of log files and/or CCTV tapes. The purpose of a silent alarm is to bring authorized security personnel to the location of the intrusion or attack in hopes of catching the person(s) committing the unwanted or unauthorized acts.

Local alarm systems must broadcast an audible (up to 120 decibel, or db) alarm signal that can be easily heard up to 400 feet away. Additionally, they must be protected from tampering and disablement, usually by security guards. For a local alarm system to be effective, there must be a security team or guards positioned nearby who can respond when the alarm is triggered. A *centralized alarm system* may not have a local alarm; a remote or centralized monitoring station is signaled when the alarm is triggered. *Auxiliary alarm systems* can be added to either local or centralized alarm systems. The purpose of an auxiliary alarm system is to notify local police or fire services when an alarm is triggered.

Secondary Verification Mechanisms

When motion detectors, sensors, and alarms are used, secondary verification mechanisms should be in place. As the sensitivity of these devices increases, false triggers occur more often. Innocuous events such as the presence of animals, birds, bugs, or authorized personnel can trigger false alarms. Deploying two or more detection and sensor systems and requiring two or more triggers in quick succession to occur before an alarm is issued may significantly reduce false alarms and increase the certainty of sensing actual intrusions or attacks.

CCTV is a security mechanism related to motion detectors, sensors, and alarms. However, CCTV is not an automated detection-and-response system. CCTV requires personnel to watch the captured video to detect suspicious and malicious activities and to trigger alarms. Security cameras can expand the effective visible range of a security guard, therefore increasing the scope of the oversight. In many cases, CCTV is not used as a primary detection tool because of the high cost of paying a person to sit and watch the video screens. Instead, it is used as a secondary or follow-up mechanism that is reviewed after a trigger from an automated system occurs. In fact, the same logic used for auditing and audit trails is used for CCTV and recorded events. A CCTV is a preventative measure, while reviewing recorded events is a detective measure.

Secondary Verification

As illustrated in the previous real-world scenario, Gino was at constant risk of security breaches because Elise is constantly forgetting (and therefore writes down) every password, while Francis is habitually forgetful about the location of his key card. What happens when someone else comes into possession of either of these items and has knowledge of how or where to use them?

Gino’s biggest advantage will be any secondary verification mechanisms he has established in the workplace. This may include a CCTV that identifies the face of the person who uses a key card for access or inputs a combination in some area designated under surveillance. Even videotape logs of ingress and egress through checkpoints can be helpful when it comes to chasing down accidental or deliberate access abuses.

With known “problem users” or “problem identities,” many security systems can issue notifications or alerts when those identities are used. Depending on the systems that are available, and the risks that unauthorized access could pose, human follow-up may or may not be warranted. But any time Elise (or somebody who uses that identity) logs onto a system or any time Francis’s key card is used, a floating or roving security guard could be dispatched to ensure that everything is on the up and up. Of course, it’s probably also a good idea to have Elise’s and Francis’s managers counsel them on the appropriate use (and storage) of passwords and key cards, just to make sure they understand the potential risks involved too.

Technical Controls

Technical controls most often employed as access control mechanisms to manage physical access include smart/dumb cards and biometrics. In addition to such controls, audit trails, access logs, and intrusion detection systems (IDSs) can serve as physical security mechanisms.

Smart Cards

Smart cards are credit-card-sized IDs, badges, or security passes with an embedded magnetic strip, bar code, or integrated circuit chip. They can contain information about the authorized bearer that can be used for identification and/or authentication purposes. Some smart cards can even process information or store reasonable amounts of data in a memory chip. A smart card may be known by several phrases or terms:

- An identity token containing integrated circuits (ICs)
- A processor IC card
- An IC card with an ISO 7816 interface

Smart cards are often viewed as a complete security solution, but they should not be considered complete by themselves. As with any single security mechanism, smart cards are subject to weaknesses and vulnerabilities. Smart cards can fall prey to physical attacks, logical attacks, Trojan horse attacks, or social-engineering attacks.

Memory cards are machine-readable ID cards with a magnetic strip. Like a credit card, debit card, or ATM card, memory cards can retain a small amount of data but are unable to process data like a smart card. Memory cards often function as a type of two-factor control: The card is “something you have” and its PIN “something you know.” However, memory cards are easy to copy or duplicate and are insufficient for authentication purposes in a secure environment.

Proximity Readers

In addition to smart and dumb cards, proximity readers can be used to control physical access. A *proximity reader* can be a passive device, a field-powered device, or a transponder. The proximity device is worn or held by the authorized bearer. When it passes a proximity reader, the reader is able to determine who the bearer is and whether they have authorized access. A passive device reflects or otherwise alters the electromagnetic field generated by the reader. This alteration is detected by the reader.

The passive device has no active electronics; it is just a small magnet with specific properties (like antitheft devices commonly found on DVDs). A field-powered device has electronics that activate when the device enters the electromagnetic field that the reader generates. Such devices actually generate electricity from an EM field to power themselves (such as card readers that require only that the access card be waved within inches of the reader to unlock doors). A transponder device is self-powered and transmits a signal received by the reader. This can occur consistently or only at the press of a button (like a garage door opener or car alarm keyfob).

In addition to smart/dumb cards and proximity readers, physical access can be managed with radio frequency identification (RFID) or biometric access control devices. See Chapter 1, “Accountability and Access Control,” for a description of biometric devices.

Access Abuses

No matter what form of physical access control is used, a security guard or other monitoring system must be deployed to prevent abuse, masquerading, and piggybacking. Examples of abuses of physical access controls are propping open secured doors and bypassing locks or access controls. *Masquerading*is using someone else’s security ID to gain entry into a facility. *Piggybacking* is following someone through a secured gate or doorway without being identified or authorized personally.

Audit trails and access logs are useful tools even for physical access control. They may need to be created manually by security guards. Or they can be generated automatically if sufficient automated access control mechanisms (such as smart cards and certain proximity readers) are in use. The time a subject requests entry, the result of the authentication process, and the length of time the secured gate remains open are important elements to include in audit trails and access logs. In addition to using the electronic or paper trail, consider monitoring entry points with CCTV. CCTV enables you to compare the audit trails and access logs with a visual recording of the events. Such information is critical to reconstruct the events for an intrusion, breach, or attack.

Intrusion Detection Systems

Intrusion detection systems are systems—automated or manual—designed to detect an attempted intrusion, breach, or attack; the use of an unauthorized entry point; or the occurrence of some specific event at an unauthorized or abnormal time. Intrusion detection systems used to monitor physical activity may include security guards, automated access controls, and motion detectors as well as other specialty monitoring techniques.

Physical intrusion detection systems, also called *burglar alarms*, detect unauthorized activities and notify the authorities (internal security or external law enforcement). Physical intrusion detection systems can monitor for vibrations, movement, temperature changes, sound, changes in electromagnetic fields, and much more. The most common type of system uses a simple circuit (aka dry contact switches) comprising foil tape in entrance points to detect when a door or window has been opened.

An intrusion detection mechanism is useful only if it is connected to an intrusion alarm. An intrusion alarm notifies authorities about a breach of physical security. There are four types of alarms:

Local alarm system An alarm sounds locally and can be heard up to 400 feet away.

Central station system The alarm is silent locally, but offsite monitoring agents are notified so they can respond to the security breach. Most residential security systems are of this type. Most central station systems are well-known or national security companies, such as Brinks and ADT.

Proprietary system This is the same thing as a central station system; however, the host organization has its own onsite security staff waiting to respond to security breaches.

Auxiliary station When the security perimeter is breached, emergency services are notified to respond to the incident and arrive at the location. This could include fire, police, and medical services.

Two or more of these types of intrusion and alarm systems can be incorporated in a single solution. However, there are two aspects of any intrusion detection and alarm system that can cause it to fail: how it gets its power and how it communicates. If the system loses power, it will not function. Thus, a reliable detection and alarm system has a battery backup with enough stored power for 24 hours of operation.

If communication lines are cut, an alarm may not function and security personnel and emergency services will not be notified. Thus, a reliable detection and alarm system incorporates a *heartbeat sensor* for line supervision. A heartbeat sensor is a mechanism by which the communication pathway is either constantly or periodically checked with a test signal. If the receiving station detects a failed heartbeat signal, the alarm triggers automatically. Both measures are designed to prevent intruders from circumventing the detection and alarm system.

Emanation Security

Many electrical devices emanate electrical signals or radiation that can be intercepted by unauthorized individuals. These signals may contain confidential, sensitive, or private data. Obvious examples of emanation devices are wireless networking equipment and mobile phones, but many other devices are vulnerable to interception. Other examples include monitors, modems, and internal or external media drives (hard drives, floppy drives, CDs, and so on). With the right equipment, unauthorized users can intercept electromagnetic or radio frequency signals (collectively known as *emanations*) from these devices and interpret them to extract confidential data.

TEMPEST

Clearly, if a device emits a signal that someone outside your organization can intercept, some security protection is needed. The types of countermeasures and safeguards used to protect against emanation attacks are known as TEMPEST countermeasures. TEMPEST was originally a government research study aimed at protecting electronic equipment from the electromagnetic pulse (EMP) emitted during nuclear explosions. It has since expanded to a general study of monitoring emanations and preventing their interception. Thus, TEMPEST is now a formal name for a broad category of activities.

Countermeasures

TEMPEST countermeasures include Faraday cages, white noise, and control zones. A *Faraday cage* is a box, mobile room, or entire building designed with an external metal skin, often a wire mesh that fully surrounds an area on all sides (in other words, front, back, left, right, top, and bottom). This metal skin is slightly electrified to produce a capacitor-like effect (which is why it’s named after Faraday, a pioneer in the field of electromagnetism) that prevents electromagnetic signals (emanations) from exiting or entering the area that the cage encloses. Faraday cages are quite effective at blocking EM signals. In fact, inside an active Faraday cage, mobile phones do not work, and you can’t pick up broadcast radio or television stations.

White noise simply means broadcasting false traffic at all times to mask and hide the presence of real emanations. White noise can consist of a real signal from another source that is not confidential, a constant signal at a specific frequency, a randomly variable signal (such as the white noise heard between radio stations or television stations), or even a jam signal that causes interception equipment to fail. White noise is most effective when created around the perimeter of an area so that it is broadcast outward to protect the internal area where emanations may be needed for normal operations.

NOTE

White noise describes any random sound, signal, or process that can drown out meaningful information. This can vary from audible frequencies to inaudible electronic transmissions, and it may even involve the deliberate act of creating line or traffic noise to disguise origins or disrupt listening devices.

A third type of TEMPEST countermeasure, a *control zone*, is simply the implementation of either a Faraday cage or white noise generation in an environment where a specific area is protected while the rest is not. A control zone can be a room, a floor, or an entire building. Control zones are those areas where emanation signals are supported and used by necessary equipment, such as wireless networking, mobile phones, radios, and televisions. Outside the control zones, emanation interception is blocked or prevented through the use of various TEMPEST countermeasures.

Environment and Life Safety

An important aspect of physical access control and maintaining the security of a facility is protecting the basic elements of the environment and protecting human life. In all circumstances and under all conditions, the most important aspect of security is protecting people. Thus, preventing harm to people is the most important goal for all security solutions.

Personnel Safety

Part of maintaining safety for personnel is maintaining the basic environment of a facility. For short periods of time, people can survive without water, food, air conditioning, and power. But in some cases, the loss of these elements can have disastrous results, or they can be symptoms of more immediate and dangerous problems. Flooding, fires, release of toxic materials, and natural disasters all threaten human life as well as the stability of a facility. Physical security procedures should focus on protecting human life and then on restoring the safety of the environment and restoring the utilities necessary for the IT infrastructure to function.

People should always be your top priority. Only after personnel are safe can you consider addressing business continuity. Many organizations adopt occupant emergency plans (OEPs) to guide and assist with sustaining personnel safety in the wake of a disaster. The OEP provides guidance on how to minimize threats to life, prevent injury, and protect property from damage in the event of a destructive physical event. The OEP does not address IT issues or business continuity, just personnel and general property. The BCP and DRP address IT and business continuity and recovery issues.

Power and Electricity

Power supplied by electric companies is not always consistent and clean. Most electronic equipment demands clean power to function properly. Equipment damage from power fluctuations is a common occurrence. Many organizations opt to manage their own power through various means. An *uninterruptible power supply (UPS)* is a type of self-charging battery that can be used to supply consistent clean power to sensitive equipment. Basically, a UPS functions by taking power in from the wall outlet, storing it in a battery, pulling power out of the battery, and then feeding that power to whatever devices are connected to it. By directing current through its battery, it is able to maintain a consistent clean power supply. A UPS has a second function, one that is often used as a selling point: A UPS provides continuous power even after the primary power source fails. A UPS can continue to supply power for minutes or hours, depending on its capacity and how much power the equipment attached to it needs.

Another means to ensure that equipment is not harmed by power fluctuations requires use of power strips with surge protectors. A surge protector includes a fuse that will blow before power levels change enough to cause damage to equipment. However, once a surge protector's fuse or circuit is tripped, current flow is completely interrupted. Surge protectors should be used only when instant termination of electricity will not cause damage or loss to the equipment. Otherwise, a UPS should be employed instead.

If maintaining operations for considerable time in spite of a brownout or blackout is a necessity, onsite electric generators are required. Such generators turn on automatically when a power failure is detected. Most generators operate using a fuel tank of liquid or gaseous propellant that must be maintained to ensure reliability. Electric generators are considered alternate or backup power sources.

The problems with power are numerous. Here is a list of terms associated with power issues you should know:

Fault A momentary loss of power

Blackout A complete loss of power

Sag Momentary low voltage

Brownout Prolonged low voltage

Spike Momentary high voltage

Surge Prolonged high voltage

Inrush An initial surge of power usually associated with connecting to a power source, whether primary or alternate/secondary

Noise A steady interfering power disturbance or fluctuation

Transient A short duration of line noise disturbance

Clean Nonfluctuating pure power

Ground The wire in an electrical circuit that is grounded

A brownout is an interesting power issue because its definition references ANSI standards for power. Those standards allow for an 8 percent drop in power between the power source and the facility meter and a drop of 3.5 percent between the facility meter and the wall outlet before any prolonged instance of low voltage is labeled as a brownout. The ANSI standard further distinguishes that low voltage outside your meter is to be repaired by the power company, while an internal brownout is your responsibility.

Noise

Noise can cause more than just problems with how equipment functions; it can also interfere with the quality of communications, transmissions, and playback. Noise generated by electric current can affect any means of data transmission that relies on electromagnetic transport mechanisms, such as telephone, cellular, television, audio, radio, and network mechanisms.

There are two types of *electromagnetic interference (EMI)*: common mode and traverse mode. *Common mode noise* is generated by a difference in power between the hot and ground wires of a power source or operating electrical equipment. *Traverse mode noise* is generated by a difference in power between the hot and neutral wires of a power source or operating electrical equipment.

Radio frequency interference (RFI) is another source of noise and interference that can affect many of the same systems as EMI. A wide range of common electrical appliances generate RFI, including fluorescent lights, electrical cables, electric space heaters, computers, elevators, motors, and electric magnets, so it’s important to locate all such equipment when deploying IT systems and infrastructure elements.

Protecting your power supply and your equipment from noise is an important part of maintaining a productive and functioning environment for your IT infrastructure. Steps to take for this kind of protection include providing for sufficient power conditioning, establishing proper grounding, shielding all cables, and limiting exposure to EMI and RFI sources.

Temperature, Humidity, and Static

In addition to power considerations, maintaining the environment involves control over the HVAC mechanisms. Rooms intended primarily to house computers should be kept at 60 to 75 degrees Fahrenheit (15 to 23 degrees Celsius). Humidity in a computer room should be maintained between 40 and 60 percent. Too much humidity can cause corrosion. Too little humidity causes static electricity. Even on nonstatic carpeting, if the environment has low humidity, it is still possible to generate 20,000-volt static discharges. As you can see in TABLE 19.1, even minimal levels of static discharge can destroy electronic equipment.

Table 19.1 Static voltage and damage

Static Voltage	**Possible Damage**
40	Destruction of sensitive circuits and other electronic components
1,000	Scrambling of monitor displays
1,500	Destruction of data stored on hard drives
2,000	Abrupt system shutdown
4,000	Printer jam or component damage

17,000	Permanent circuit damage

Water

Water leakage and flooding should be addressed in your environmental safety policy and procedures. Plumbing leaks are not an everyday occurrence, but when they do happen, they can cause significant damage.

Water and electricity don't mix. If your computer systems come in contact with water, especially while they are operating, damage is sure to occur. Plus, water and electricity create a serious risk of electrocution for nearby personnel. Whenever possible, locate server rooms and critical computer equipment away from any water source or transport pipes. You may also want to install water detection circuits on the floor around mission-critical systems. Water detection circuits will sound an alarm and alert you if water is encroaching upon the equipment.

To minimize emergencies, be familiar with shutoff valves and drainage locations. In addition to monitoring for plumbing leaks, you should evaluate your facility's ability to handle severe rain or flooding in its vicinity. Is the facility located on a hill or in a valley? Is there sufficient drainage? Is there a history of flooding or accumulation of standing water? Is a server room in the basement or on the first floor?

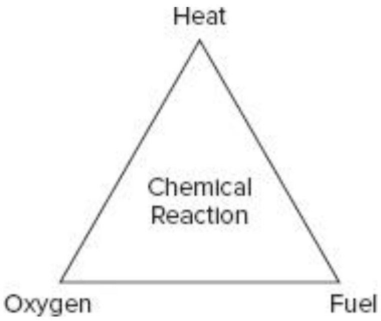
Fire Detection and Suppression

Fire detection and suppression must not be overlooked. Protecting personnel from harm should always be the most important goal of any security or protection system. In addition to protecting people, fire detection and suppression is designed to keep damage caused by fire, smoke, heat, and suppression materials to a minimum, especially as regards the IT infrastructure.

Basic fire education involves knowledge of the fire triangle (see Figure 19.2). The three corners of the triangle represent fire, heat, and oxygen. The center of the triangle represents the chemical reaction among these three elements. The point of the fire triangle is to illustrate that if you can remove any one of the four items from the fire triangle, the fire can be extinguished. Different suppression mediums address different aspects of the fire:

- Water suppresses the temperature.
- Soda acid and other dry powders suppress the fuel supply.
- CO_2 suppresses the oxygen supply.
- Halon substitutes and other nonflammable gases interfere with the chemistry of combustion and/or suppress the oxygen supply.

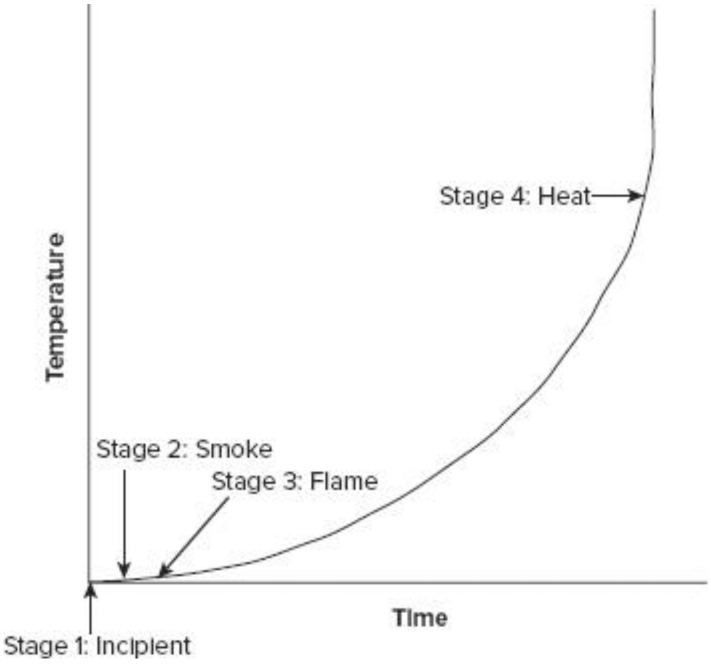
FIGURE 19.2 The fire triangle



When selecting a suppression medium, it is important to consider what aspect of the fire triangle it addresses, what this really represents, how effective the suppression medium usually is, and what impact the suppression medium will exert on your environment.

In addition to understanding the fire triangle, it is also helpful to understand the stages of fire. Fires go through numerous stages, and Figure 19.3 addresses the four most vital stages.

FIGURE 19.3 The four primary stages of fire



Stage 1: The incipient stage At this stage, there is only air ionization but no smoke.

Stage 2: The smoke stage In Stage 2, smoke is visible from the point of ignition.

Stage 3: The flame stage This is when a flame can be seen with the naked eye.

Stage 4: The heat stage At Stage 4, the fire is considerably further down the timescale to the point where there is an intense heat buildup and everything in the area burns.

The earlier a fire is detected, the easier it is to extinguish and the less damage it and its suppression medium(s) can cause.

One of the basics of fire management is proper personnel awareness training. Everyone should be thoroughly familiar with the fire suppression mechanisms in their facility. Everyone should also be familiar with at least two evacuation routes from their primary work area and know how to locate evacuation routes elsewhere in the facility. Personnel should be trained in the location and use of fire extinguishers. Other items to include in fire or general emergency-response training include cardiopulmonary resuscitation (CPR), emergency shutdown procedures, and a preestablished rendezvous location or safety verification mechanism (such as voicemail).

TIP

Most fires in a data center are caused by overloaded electrical distribution outlets.

Fire Extinguishers

There are several types of fire extinguishers. Understanding what type to use on various forms of fire is essential to effective fire suppression. If a fire extinguisher is used improperly or the wrong form of fire extinguisher is used, the fire could spread and intensify instead of being quenched. Fire extinguishers are to be used only when a fire is still in the incipient stage. TABLE 19.2 lists the three common types of fire extinguishers.

Table 19.2 Fire extinguisher classes

Class	Type	Suppression Material
A	Common combustibles	Water, soda acid (a dry powder or liquid chemical)
B	Liquids	CO_2, halon*, soda acid
C	Electrical	CO_2, halon*
D	Metal	Dry powder

*Halon or an EPA-approved halon substitute

TIP

Water cannot be used on Class B fires because it splashes the burning liquids and such liquids usually float. Water cannot be used on Class C fires because of the potential for electrocution. Oxygen suppression cannot be used on metal fires because burning metal produces its own oxygen.

Fire Detection Systems

To properly protect a facility from fire requires installing an automated detection and suppression system. There are many types of fire detection systems. Fixed-temperature detection systems trigger suppression when a specific temperature is reached. The trigger is usually a metal or plastic component that is in the sprinkler head and melts at a specific temperature. Rate-of-rise detection systems trigger suppression when the speed at which the temperature changes reaches a specific level. Flame-actuated systems trigger suppression based on the infrared energy of flames. Smoke-actuated systems use photoelectric or radioactive ionization sensors as triggers.

Most fire detection systems can be linked to fire response service notification mechanisms. When suppression is triggered, such linked systems will contact the local fire response team and request aid using an automated message or alarm.

To be effective, fire detectors need to be placed strategically. Don't forget to place them inside dropped ceilings and raised floors, in server rooms, in private offices and public areas, in HVAC vents, in elevator shafts, in the basement, and so on.

As for suppression mechanisms used, they can be based on water or on a fire suppression gas system. Water is common in human-friendly environments, whereas gaseous systems are more appropriate for computer rooms where personnel typically do not reside.

Water Suppression Systems

There are four main types of water suppression systems.

- A *wet pipe system* (also known as a *closed head system*) is always full of water. Water discharges immediately when suppression is triggered.
- A *dry pipe system* contains compressed air. Once suppression is triggered, the air escapes, opening a water valve that in turn causes the pipes to fill and discharge water into the environment.
- A *deluge system* is another form of dry pipe system that uses larger pipes and therefore delivers a significantly larger volume of water. Deluge systems are inappropriate for environments that contain electronics and computers.

- A *preaction system* is a combination dry pipe/wet pipe system. The system exists as a dry pipe until the initial stages of a fire (smoke, heat, and so on) are detected, and then the pipes are filled with water. The water is released only after the sprinkler head activation triggers are melted by sufficient heat. If the fire is quenched before sprinklers are triggered, pipes can be manually emptied and reset. This also allows manual intervention to stop the release of water before sprinkler triggering occurs.

Preaction systems are the most appropriate water-based system for environments that house both computers and humans together.

TIP

> The most common cause of failure for a water-based system is human error, such as turning off a water source when a fire occurs or triggering water release when there is no fire.

Gas Discharge Systems

Gas discharge systems are usually more effective than water discharge systems. However, gas discharge systems should not be used in environments in which people are located. Gas discharge systems usually remove the oxygen from the air, thus making them hazardous to personnel. They employ a pressurized gaseous suppression medium, such as CO_2, halon, or FM-200 (a halon replacement).

Halon is an effective fire suppression compound, but it degrades into toxic gases at 900 degrees Fahrenheit. Also, it is not environmentally friendly. The EPA has banned the manufacture of halon in the United States, but it can still be imported into that country. However, according to the Montreal Protocol, you should contact a halon recycling facility to make arrangements for refilling a discharged system instead of contacting a vendor or manufacturer directly. This action is encouraged so that already produced halon will be consumed and less new halon will be manufactured.

Owing to issues with halon, it is often replaced by a more ecologically friendly and less toxic medium. The following list itemizes various EPA-approved substitutes for halon:

- FM-200 (HFC-227ea)
- CEA-410 or CEA-308
- NAF-S-III (HCFC Blend A)

- FE-13 (HCFC-23)
- Argon (IG55) or Argonite (IG01)
- Inergen (IG541)

You can also replace halon substitutes with low-pressure water mists, but such systems are usually not employed in computer rooms or electrical equipment storage facilities. A low-pressure water mist is a vapor cloud used to quickly reduce the temperature in an area.

Damage

Addressing fire detection and suppression includes dealing with possible contamination and damage caused by a fire. The destructive elements of a fire include smoke and heat, but they also include the suppression media, such as water or soda acid. Smoke is damaging to most storage devices. Heat can damage any electronic or computer component. For example, temperatures of 100 degrees Fahrenheit can damage storage tapes, 175 degrees can damage computer hardware (that is, CPU and RAM), and 350 degrees can damage paper products (through warping and discoloration).

Suppression media can cause short circuits, initiate corrosion, or otherwise render equipment useless. All these issues must be addressed when designing a fire response system.

WARNING

> Don’t forget that in the event of a fire, in addition to damage caused by the flames and your chosen suppression medium, members of the fire department may inflict damage using their hoses to spray water and their axes while searching for hot spots.

Equipment Failure

No matter what the quality of the equipment your organization chooses to purchase and install might be, eventually it will fail. Understanding and preparing for this eventuality helps ensure the ongoing availability of your IT infrastructure and should help you to protect the integrity and availability of your resources.

Preparing for equipment failure can take many forms. In some non-mission-critical situations, simply knowing where you can purchase replacement parts for a 48-hour replacement timeline is sufficient. In other situations, maintaining onsite replacement parts is mandatory. Keep in mind that the response time in returning a system to a fully functioning state is directly proportional to the cost involved in maintaining such a solution. Costs include storage, transportation, prepurchasing, and maintaining onsite installation and restoration expertise. In some cases, maintaining onsite replacements is infeasible. For those cases, establishing a service-level agreement (SLA) with the hardware vendor is essential. An SLA clearly defines the response time a vendor will provide in the event of an equipment failure emergency.

Aging hardware should be scheduled for replacement and/or repair. The schedule for such operations should be based on the mean time to failure (MTTF) and mean time to repair (MTTR) estimates established for each device or upon prevailing best organizational practices for managing the hardware lifecycle. MTTF is the expected typical functional lifetime of the device given a specific operating environment. MTTR is the average length of time required to perform a repair on the device. A device can often undergo numerous repairs before a catastrophic failure is expected. Be sure to schedule all devices to be replaced before their MTTF expires.

When a device is sent out for repairs, you need to have an alternate solution or a backup device to fill in for the duration of the repair time. Often, waiting until a minor failure occurs before a repair is performed is satisfactory, but waiting until a complete failure occurs before replacement is an unacceptable security practice.

Summary

If you don’t have control over the physical environment, no amount of administrative or technical/logical access controls can provide adequate security. If a malicious person can gain physical access to your facility or equipment, they own it.

There are many aspects and elements involved in implementing and maintaining physical security. One core element is selecting or designing the facility to house your IT infrastructure and the operations of your organization. You must start with a plan that outlines the security needs for your organization and emphasizes methods or mechanisms to employ to provide such security. Such a plan is developed through a process known as *critical path analysis*.

The security controls implemented to manage physical security can be divided into three groups: administrative, technical, and physical. Administrative physical security controls include facility construction and selection, site management, personnel controls, awareness training, and emergency response and procedures. Technical physical security controls include access controls, intrusion detection, alarms, CCTV, monitoring, HVAC, power supplies, and fire detection and suppression. Examples of physical controls for physical security include fencing, lighting, locks, construction materials, mantraps, dogs, and guards.

There are many types of physical access control mechanisms that can be deployed in an environment to control, monitor, and manage access to a facility. These range from deterrents to detection mechanisms. They can be fences, gates, turnstiles, mantraps, lighting, security guards, security dogs, key locks, combination locks, badges, motion detectors, sensors, and alarms.

The technical controls most often employed as access control mechanisms to manage physical access include smart/dumb cards and biometrics. In addition to access control, physical security mechanisms can take the form of audit trails, access logs, and intrusion detection systems.

An important aspect of physical access control and maintaining the security of a facility is protecting the basic elements of the environment and protecting human life. In all circumstances and under all conditions, the most important goal of security is protecting people. Preventing harm is the utmost goal of all security solutions. Providing clean power sources and managing the environment are also important.

Fire detection and suppression must not be overlooked. In addition to protecting people, fire detection and suppression is designed to keep damage caused by fire, smoke, heat, and suppression materials to a minimum, especially in regard to the IT infrastructure.

Exam Essentials

Understand why there is no security without physical security. Without control over the physical environment, no amount of administrative or technical/logical access controls can provide adequate security. If a malicious person can gain physical access to your facility or equipment, they can do just about anything they want, from destruction to disclosure and alteration.

Be able to list administrative physical security controls. Examples of administrative physical security controls are facility construction and selection, site management, personnel controls, awareness training, and emergency response and procedures.

Be able to list the technical physical security controls. Technical physical security controls can be access controls, intrusion detection, alarms, CCTV, monitoring, HVAC, power supplies, and fire detection and suppression.

Be able to name the physical controls for physical security. Physical controls for physical security are fencing, lighting, locks, construction materials, mantraps, dogs, and guards.

Know the functional order of controls. These are denial, then deterrence, then detection, and then delay.

Know the key elements in making a site selection and designing a facility for construction. The key elements in making a site selection are visibility, composition of the surrounding area, area accessibility, and the effects of natural disasters. A key element in designing a facility for construction is understanding the level of security needed by your organization and planning for it before construction begins.

Know how to design and configure secure work areas. There should not be equal access to all locations within a facility. Areas that contain assets of higher value or importance should have restricted access. Valuable and confidential assets should be located in the heart or center of protection provided by a facility. Also, centralized server or computer rooms need not be human compatible.

Understand how to handle visitors in a secure facility. If a facility employs restricted areas to control physical security, then a mechanism to handle visitors is required. Often an escort is assigned to visitors, and their access and activities are monitored closely. Failing to track the actions of outsiders when they are granted access into a protected area can result in malicious activity against the most protected assets.

Know the three categories of security controls implemented to manage physical security and be able to name examples of each. The security controls implemented to manage physical security can be divided into three groups: administrative, technical, and physical. Understand when and how to use each, and be able to list examples of each kind.

Know the common threats to physical access controls. No matter what form of physical access control is used, a security guard or other monitoring system must be deployed to prevent abuse, masquerading, and piggybacking. Abuses of physical access control are propping open secured doors and bypassing locks or access controls. Masquerading is using someone else's security ID to gain entry into a facility. Piggybacking is following someone through a secured gate or doorway without being identified or authorized personally.

Understand the need for audit trails and access logs. Audit trails and access logs are useful tools even for physical access control. They may need to be created manually by security guards. Or they can be generated automatically if sufficiently automated access control mechanisms are in place (in other words, smart cards and certain proximity readers). You should also consider monitoring entry points with CCTV. Through CCTV, you can compare the audit trails and access logs with a visually recorded history of the events. Such information is critical to reconstructing the events of an intrusion, breach, or attack.

Understand the need for clean power. Power supplied by electric companies is not always consistent and clean. Most electronic equipment demands clean power in order to function properly. Equipment damage because of power fluctuations is a common occurrence. Many organizations opt to manage their own power through several means. A UPS is a type of self-charging battery that can be used to supply consistent clean power to sensitive equipment. UPSs also provide continuous power even after the primary power source fails. A UPS can continue to supply power for minutes or hours depending on its capacity and the draw by equipment.

Know the terms commonly associated with power issues. Know the definitions of the following: fault, blackout, sag, brownout, spike, surge, inrush, noise, transient, clean, and ground.

Understand how to control the environment. In addition to power considerations, maintaining the environment involves control over the HVAC mechanisms. Rooms containing primarily computers should be kept at 60 to 75 degrees Fahrenheit (15 to 23 degrees Celsius). Humidity in a computer room should be maintained between 40 and 60 percent. Too much humidity can cause corrosion. Too little humidity causes static electricity.

Know about static electricity. Even on nonstatic carpeting, if the environment has low humidity, it is still possible to generate 20,000-volt static discharges. Even minimal levels of static discharge can destroy electronic equipment.

Understand the need to manage water leakage and flooding. Water leakage and flooding should be addressed in your environmental safety policy and procedures. Plumbing leaks are not an everyday occurrence, but when they occur, they often cause significant damage. Water and electricity don't mix. If your computer systems come in contact with water, especially while they are operating, damage is sure to occur. Whenever possible, locate server rooms and critical computer equipment away from any water source or transport pipes.

Understand the importance of fire detection and suppression. Fire detection and suppression must not be overlooked. Protecting personnel from harm should always be the most important goal of any security or protection system. In addition to protecting people, fire detection and suppression is designed to keep damage caused by fire, smoke, heat, and suppression materials to a minimum, especially in regard to the IT infrastructure.

Understand the possible contamination and damage caused by a fire and suppression. The destructive elements of a fire include smoke and heat but also the suppression medium, such as water or soda acid. Smoke is damaging to most storage devices. Heat can damage any electronic or computer component. Suppression mediums can cause short circuits, initiate corrosion, or otherwise render equipment useless. All of these issues must be addressed when designing a fire response system.

Written Lab

1. What kind of device helps to define an organization's perimeter, and also serves to deter casual trespassing?

2. What is the problem with halon-based fire suppression technology?

3. What kinds of potential issues can an emergency visit from the fire department leave in its wake?

Answers to Written Lab

1. A fence is an excellent perimeter safeguard that can help to deter casual trespassing. Moderately secure installations work when the fence is 6 to 8 feet tall and will typically be cyclone (also known as chain link) fencing with the upper surface twisted or barbed to deter casual climbers. More secure installations usually opt for fence heights over 8 feet and often include multiple strands of barbed or razor wire strung above the chain link fabric to further deter climbers.

2. Although you will often see fire suppression information and texts reference fire suppression systems based on halon gas, which serve to starve a fire of oxygen by disrupting the chemical reaction between oxygen and combustible materials, halon is no longer approved by the U.S. EPA for new fire suppression systems, nor is manufacture of new halon gas encouraged for charging of such systems (the EPA seeks to exhaust existing stocks of halon to take this substance out of circulation). Halon is an ozone depleting substance, and production of halon 1301, halon 1211, and halon 2403 ceased in developed countries on December 31, 2003. Inert gases (such as nitrogen or argon), halocarbon gases (FE-13, FE-125, FM-200, FE-36, CEA-308, and CEA-410), and halocarbon generators are all recommended as substitutes. See http://www.berr.gov.uk/files/file29105.pdf for more information.

3. Any time water is used to respond to fire, flame, or smoke, water damage becomes a serious concern, particularly when water is released in areas where electrical equipment is in use. Not only can computers and other electrical gear be damaged or destroyed by water, so also can many forms of storage media become damaged or unusable. Also, when seeking hot spots to put out, firefighters often use axes to break down doors or cut through walls to reach them as quickly as possible. This, too, poses the potential for physical damage to or destruction of devices and/or wiring that may also be in the vicinity.

Review Questions

1. Which of the following is the most important aspect of security?

A. Physical security

B. Intrusion detection

C. Logical security

D. Awareness training

2. What method can be used to map out the needs of an organization for a new facility?

A. Log file audit

B. Critical path analysis

C. Risk analysis

D. Inventory

3. What type of physical security controls focus on facility construction and selection, site management, personnel controls, awareness training, and emergency response and procedures?

A. Technical

B. Physical

C. Administrative

D. Logical

4. Which of the following is not a security-focused design element of a facility or site?

A. Separation of work and visitor areas

B. Restricted access to areas with higher value or importance

C. Confidential assets located in the heart or center of a facility

D. Equal access to all locations within a facility

5. Which of the following does not need to be true in order to maintain the most efficient and secure server room?

A. It must be human compatible.

B. It must include the use of nonwater fire suppressants.

C. The humidity must be kept between 40 and 60 percent.

D. The temperature must be kept between 60 and 75 degrees Fahrenheit.

6. What is a perimeter-defining device used to deter casual trespassing?

A. Gates

B. Fencing

C. Security guards

D. Motion detectors

7. Which of the following is a double set of doors that is often protected by a guard and is used to contain a subject until their identity and authentication is verified?

A. Gate

B. Turnstile

C. Mantrap

D. Proximity detector

8. What is the most common form of perimeter security devices or mechanisms?

A. Security guards

B. Fences

C. CCTV

D. Lighting

9. Which of the following is not a disadvantage of using security guards?

A. Security guards are usually unaware of the scope of the operations within a facility.

B. Not all environments and facilities support security guards.

C. Not all security guards are themselves reliable.

D. Prescreening, bonding, and training do not guarantee effective and reliable security guards.

10. What is the most common cause of failure for a water-based fire suppression system?

A. Water shortage

B. People

C. Ionization detectors

D. Placement of detectors in drop ceilings

11. What is the most common and inexpensive form of physical access control device?

A. Lighting

B. Security guard

C. Key locks

D. Fences

12. What type of motion detector senses changes in the electrical or magnetic field surrounding a monitored object?

A. Wave

B. Photoelectric

C. Heat

D. Capacitance

13. Which of the following is not a typical type of alarm that can be triggered for physical security?

A. Preventive

B. Deterrent

C. Repellant

D. Notification

14. No matter what form of physical access control is used, a security guard or other monitoring system must be deployed to prevent all but which of the following?

A. Piggybacking

B. Espionage

C. Masquerading

D. Abuse

15. What is the most important goal of all security solutions?

A. Prevention of disclosure

B. Maintaining integrity

C. Human safety

D. Sustaining availability

16. What is the ideal humidity range for a computer room?

A. 20–40 percent

B. 40–60 percent

C. 60–75 percent

D. 80–95 percent

17. At what voltage level can static electricity cause destruction of data stored on hard drives?

- **A.** 4,000
- **B.** 17,000
- **C.** 40
- **D.** 1,500

18. A Type B fire extinguisher may use all but which of the following suppression mediums?

- **A.** Water
- **B.** CO_2
- **C.** Halon or an acceptable halon substitute
- **D.** Soda acid

19. What is the best type of water-based fire suppression system for a computer facility?

- **A.** Wet pipe system
- **B.** Dry pipe system
- **C.** Preaction system
- **D.** Deluge system

20. Which of the following is typically not a culprit in causing damage to computer equipment in the event of a fire and a triggered suppression?

- **A.** Heat
- **B.** Suppression medium
- **C.** Smoke
- **D.** Light

Answers to Review Questions

1. A. Physical security is the most important aspect of overall security. Without physical security, none of the other aspects of security is sufficient.

2. B. Critical path analysis can be used to map out the needs of an organization for a new facility. A critical path analysis is the process of identifying relationships between mission-critical applications, processes, and operations and all of the supporting elements.

3. C. Administrative physical security controls include facility construction and selection, site management, personnel controls, awareness training, and emergency response and procedures.

4. D. Equal access to all locations within a facility is not a security-focused design element. Each area containing assets or resources of different importance, value, and confidentiality should have a corresponding level of security restriction placed on it.

5. A. A computer room does not need to be human compatible to be efficient and secure. Having a human-incompatible server room provides a greater level of protection against attacks.

6. B. Fencing is a perimeter-defining device used to deter casual trespassing. Gates, security guards, and motion detectors do not define a facility's perimeter.

7. C. A mantrap is a double set of doors that is often protected by a guard and used to contain a subject until their identity and authentication is verified.

8. D. Lighting is the most common form of perimeter security devices or mechanisms. Your entire site should be clearly lit. This provides for easy identification of personnel and makes it easier to notice intrusions.

9. A. Security guards are usually unaware of the scope of the operations within a facility, which supports confidentiality and helps reduce the possibility that a security guard will be involved in the disclosure of confidential information.

10. B. The most common cause of failure for a water-based system is human error. If you turn off the water source after a fire and forget to turn it back on, you'll be in trouble for the future. Also, pulling an alarm when there is no fire will trigger damaging water release throughout the office.

11. C. Key locks are the most common and inexpensive form of physical access control device. Lighting, security guards, and fences are all much more cost intensive.

12. D. A capacitance motion detector senses changes in the electrical or magnetic field surrounding a monitored object.

13. A. There is no such thing as a preventive alarm. Alarms are always triggered in response to a detected intrusion or attack.

14. B. No matter what form of physical access control is used, a security guard or other monitoring system must be deployed to prevent abuse, masquerading, and piggybacking. Espionage cannot be prevented by physical access controls.

15. C. Human safety is the most important goal of all security solutions.

16. B. The humidity in a computer room should ideally be from 40 to 60 percent.

17. D. Destruction of data stored on hard drives can be caused by 1,500 volts of static electricity.

18. A. Water is never the suppression medium in Type B fire extinguishers because they are used on liquid fires.

19. C. A preaction system is the best type of water-based fire suppression system for a computer facility.

20. D. Light is usually not damaging to most computer equipment, but fire, smoke, and the suppression medium (typically water) are very destructive.

Appendix

About the Companion CD

IN THIS APPENDIX:

- **What you'll find on the CD**
- **System requirements**
- **Using the CD**
- **Troubleshooting**

What You'll Find on the CD

The following sections are arranged by category and summarize the software and other goodies you'll find on the CD. If you need help with installing the items provided on the CD, refer to the installation instructions in the "Using the CD" section of this appendix.

Sybex Test Engine

The CD contains the Sybex test engine, which includes the two bonus exams.

Electronic Flashcards

These handy electronic flashcards are just what they sound like. One side contains a question or fill-in-the-blank, and the other side shows the answer.

PDF of the Book

We have included an electronic version of the text in `.pdf` format. You can view the electronic version of the book with Adobe Reader.

Adobe Reader

We've also included a copy of Adobe Reader so you can view PDF files that accompany the book's content. For more information on Adobe Reader or to check for a newer version, visit Adobe's website at www.adobe.com/products/reader/.

System Requirements

Make sure your computer meets the minimum system requirements, shown in the following list. If your computer doesn't match up to most of these requirements, you may have problems using the software and files on the companion CD. For the latest and greatest information, please refer to the ReadMe file located at the root of the CD-ROM.

- A PC running Microsoft Windows 98, Windows 2000, Windows NT4 (with SP4 or later), Windows Me, Windows XP, Windows Vista, or Windows 7
- An Internet connection
- A CD-ROM drive

Using the CD

To install the items from the CD to your hard drive, follow these steps:

1. Insert the CD into your computer's CD-ROM drive. The license agreement appears.

Windows users: The interface won't launch if you have autorun disabled. In that case, click Start ⇒ Run (for Windows Vista or Windows 7, Start ⇒ All Programs ⇒ Accessories ⇒ Run). In the dialog box that appears, type **`D:\Start.exe`**. (Replace *D* with the proper letter if your CD drive uses a different letter. If you don't know the letter, see how your CD drive is listed under My Computer.) Click OK.

2. Read the license agreement, and then click the Accept button if you want to use the CD.

The CD interface appears. The interface allows you to access the content with just one or two clicks.

Troubleshooting

Wiley has attempted to provide programs that work on most computers with the minimum system requirements. Alas, your computer may differ, and some programs may not work properly for some reason.

The two likeliest problems are that you don't have enough memory (RAM) for the programs you want to use or you have other programs running that are affecting installation or running of a program. If you get an error message such as "Not enough memory" or "Setup cannot continue," try one or more of the following suggestions and then try using the software again:

Turn off any antivirus software running on your computer. Installation programs sometimes mimic virus activity and may make your computer incorrectly believe that it's being infected by a virus.

Close all running programs. The more programs you have running, the less memory is available to other programs. Installation programs typically update files and programs, so if you keep other programs running, installation may not work properly.

Have your local computer store add more RAM to your computer. This is, admittedly, a drastic and somewhat expensive step. However, adding more memory can really help the speed of your computer and allow more programs to run at the same time.

Customer Care

If you have trouble with the book's companion CD-ROM, please call the Wiley Product Technical Support phone number at (800) 762-2974.

Appendix

About the Companion CD

IN THIS APPENDIX:

- **What you'll find on the CD**
- **System requirements**
- **Using the CD**
- **Troubleshooting**

What You'll Find on the CD

The following sections are arranged by category and summarize the software and other goodies you'll find on the CD. If you need help with installing the items provided on the CD, refer to the installation instructions in the "Using the CD" section of this appendix.

Sybex Test Engine

The CD contains the Sybex test engine, which includes the two bonus exams.

Electronic Flashcards

These handy electronic flashcards are just what they sound like. One side contains a question or fill-in-the-blank, and the other side shows the answer.

PDF of the Book

We have included an electronic version of the text in `.pdf` format. You can view the electronic version of the book with Adobe Reader.

Adobe Reader

We’ve also included a copy of Adobe Reader so you can view PDF files that accompany the book’s content. For more information on Adobe Reader or to check for a newer version, visit Adobe’s website at www.adobe.com/products/reader/.

System Requirements

Make sure your computer meets the minimum system requirements, shown in the following list. If your computer doesn’t match up to most of these requirements, you may have problems using the software and files on the companion CD. For the latest and greatest information, please refer to the ReadMe file located at the root of the CD-ROM.

- A PC running Microsoft Windows 98, Windows 2000, Windows NT4 (with SP4 or later), Windows Me, Windows XP, Windows Vista, or Windows 7
- An Internet connection
- A CD-ROM drive

Using the CD

To install the items from the CD to your hard drive, follow these steps:

1. Insert the CD into your computer’s CD-ROM drive. The license agreement appears.

> *Windows users*: The interface won’t launch if you have autorun disabled. In that case, click Start ⇒ Run (for Windows Vista or Windows 7, Start ⇒ All Programs ⇒ Accessories ⇒ Run). In the dialog box that appears, type **`D:\Start.exe`**. (Replace *D* with the proper letter if your CD drive uses a different letter. If you don’t know the letter, see how your CD drive is listed under My Computer.) Click OK.

2. Read the license agreement, and then click the Accept button if you want to use the CD.

The CD interface appears. The interface allows you to access the content with just one or two clicks.

Troubleshooting

Wiley has attempted to provide programs that work on most computers with the minimum system requirements. Alas, your computer may differ, and some programs may not work properly for some reason.

The two likeliest problems are that you don’t have enough memory (RAM) for the programs you want to use or you have other programs running that are affecting installation or running of a program. If you get an error message such as “Not enough memory” or “Setup cannot continue,” try one or more of the following suggestions and then try using the software again:

- **Turn off any antivirus software running on your computer.** Installation programs sometimes mimic virus activity and may make your computer incorrectly believe that it’s being infected by a virus.
- **Close all running programs.** The more programs you have running, the less memory is available to other programs. Installation programs typically update files and programs, so if you keep other programs running, installation may not work properly.
- **Have your local computer store add more RAM to your computer.** This is, admittedly, a drastic and somewhat expensive step. However, adding more memory can really help the speed of your computer and allow more programs to run at the same time.

Customer Care

If you have trouble with the book’s companion CD-ROM, please call the Wiley Product Technical Support phone number at (800) 762-2974.

Index

Wiley Publishing, Inc. End-User License Agreement

“WPI”. By opening the accompanying software packet(s), you acknowledge that you have read and accept the following terms and conditions. If you do not agree and do not want to be bound by such terms and conditions, promptly return the Book and the unopened software packet(s) to the place you obtained them for a full refund.

1. License Grant. WPI grants to you (either an individual or entity) a nonexclusive license to use one copy of the enclosed software program(s) (collectively, the “Software”) solely for your own personal or business purposes on a single computer (whether a standard computer or a workstation component of a multi-user network). The Software is in use on a computer when it is loaded into temporary memory (RAM) or installed into permanent memory (hard disk, CD-ROM, or other storage device). WPI reserves all rights not expressly granted herein.

2. Ownership. WPI is the owner of all right, title, and interest, including copyright, in and to the compilation of the Software recorded on the physical packet included with this Book “Software Media”. Copyright to the individual programs recorded on the Software Media is owned by the author or other authorized copyright owner of each program. Ownership of the Software and all proprietary rights relating thereto remain with WPI and its licensers.

3. Restrictions on Use and Transfer.

(a) You may only (i) make one copy of the Software for backup or archival purposes, or (ii) transfer the Software to a single hard disk, provided that you keep the original for backup or archival purposes. You may not (i) rent or lease the Software, (ii) copy or reproduce the Software through a LAN or other network system or through any computer subscriber system or bulletin-board system, or (iii) modify, adapt, or create derivative works based on the Software.

(b) You may not reverse engineer, decompile, or disassemble the Software. You may transfer the Software and user documentation on a permanent basis, provided that the transferee agrees to accept the terms and conditions of this Agreement and you retain no copies. If the Software is an update or has been updated, any transfer must include the most recent update and all prior versions.

4. Restrictions on Use of Individual Programs. You must follow the individual requirements and restrictions detailed for each individual program in the "About the CD" appendix of this Book or on the Software Media. These limitations are also contained in the individual license agreements recorded on the Software Media. These limitations may include a requirement that after using the program for a specified period of time, the user must pay a registration fee or discontinue use. By opening the Software packet(s), you agree to abide by the licenses and restrictions for these individual programs that are detailed in the "About the CD" appendix and/or on the Software Media. None of the material on this Software Media or listed in this Book may ever be redistributed, in original or modified form, for commercial purposes.

5. Limited Warranty.

(a) WPI warrants that the Software and Software Media are free from defects in materials and workmanship under normal use for a period of sixty (60) days from the date of purchase of this Book. If WPI receives notification within the warranty period of defects in materials or workmanship, WPI will replace the defective Software Media.

(b) WPI AND THE AUTHOR(S) OF THE BOOK DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SOFTWARE, THE PROGRAMS, THE SOURCE CODE CONTAINED THEREIN, AND/OR THE TECHNIQUES DESCRIBED IN THIS BOOK. WPI DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR FREE.

(c) This limited warranty gives you specific legal rights, and you may have other rights that vary from jurisdiction to jurisdiction.

6. Remedies.

(a) WPI's entire liability and your exclusive remedy for defects in materials and workmanship shall be limited to replacement of the Software Media, which may be returned to WPI with a copy of your receipt at the following address: Software Media Fulfillment Department, Attn.: *CISSP:Certified Information Systems Security Professional Study Guide*, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, or call 1-800-762-2974. Please allow four to six weeks for delivery. This Limited Warranty is void if failure of the Software Media has resulted from accident, abuse, or misapplication. Any replacement Software Media will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

(b) In no event shall WPI or the author be liable for any damages whatsoever (including without limitation damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising from the use of or inability to use the Book or the Software, even if WPI has been advised of the possibility of such damages.

(c) Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation or exclusion may not apply to you.

7. U.S. Government Restricted Rights. Use, duplication, or disclosure of the Software for or on behalf of the United States of America, its agencies and/or instrumentalities "U.S. Government" is subject to restrictions as stated in paragraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, or subparagraphs (c) (1) and (2) of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19, and in similar clauses in the NASA FAR supplement, as applicable.

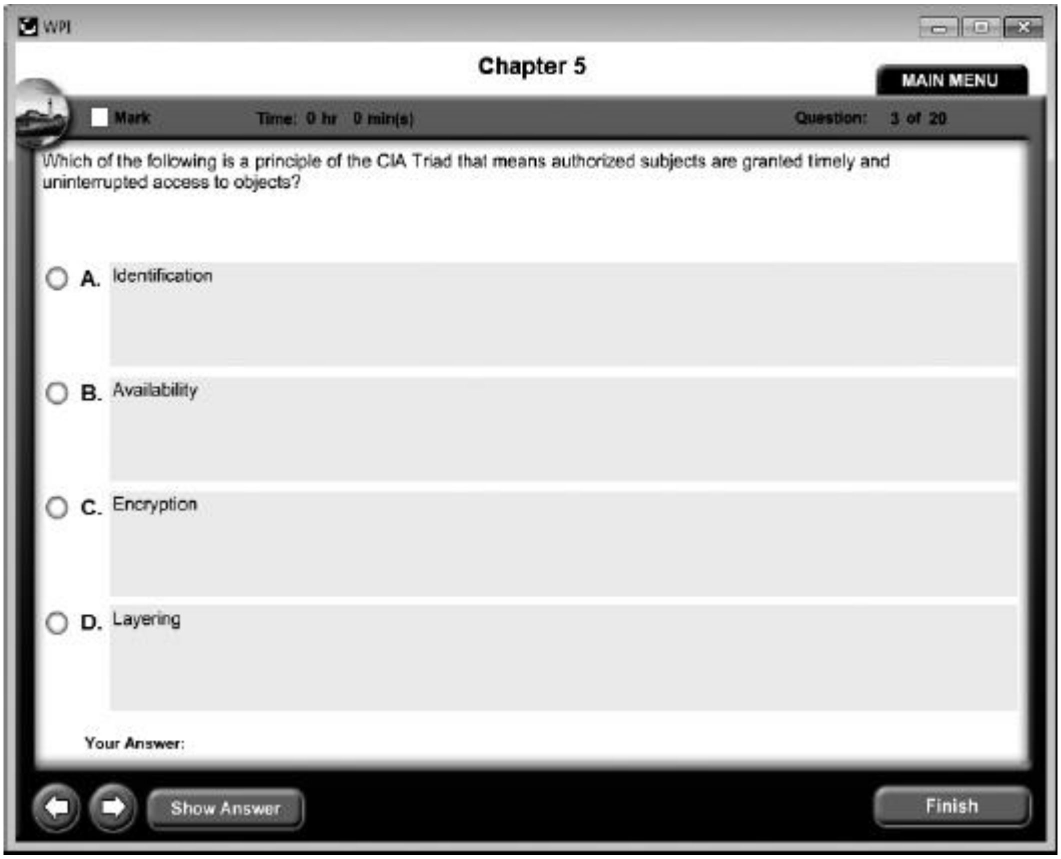
8. General. This Agreement constitutes the entire understanding of the parties and revokes and supersedes all prior agreements, oral or written, between them and may not be modified or amended except in a writing signed by both parties hereto that specifically refers to this Agreement. This Agreement shall take precedence over any other documents that may be in conflict herewith. If any one or more provisions contained in this Agreement are held by any court or tribunal to be invalid, illegal, or otherwise unenforceable, each and every other provision shall remain in full force and effect.

The Absolutely Best CISSP Book/CD Package on the Market!

Get ready for your Certified Information Systems Security Professional exam with the most comprehensive and challenging sample tests anywhere!

The Sybex Test Engine features:

- All the review questions, as covered in each chapter of the book
- Challenging questions representative of those you'll find on the real exam
- Two full-length 250-question bonus exams available only on the CD
- An Assessment Test to narrow your focus to certain objective groups.



Chapter 5

Which of the following is a principle of the CIA Triad that means authorized subjects are granted timely and uninterrupted access to objects?

○ A. Identification

○ B. Availability

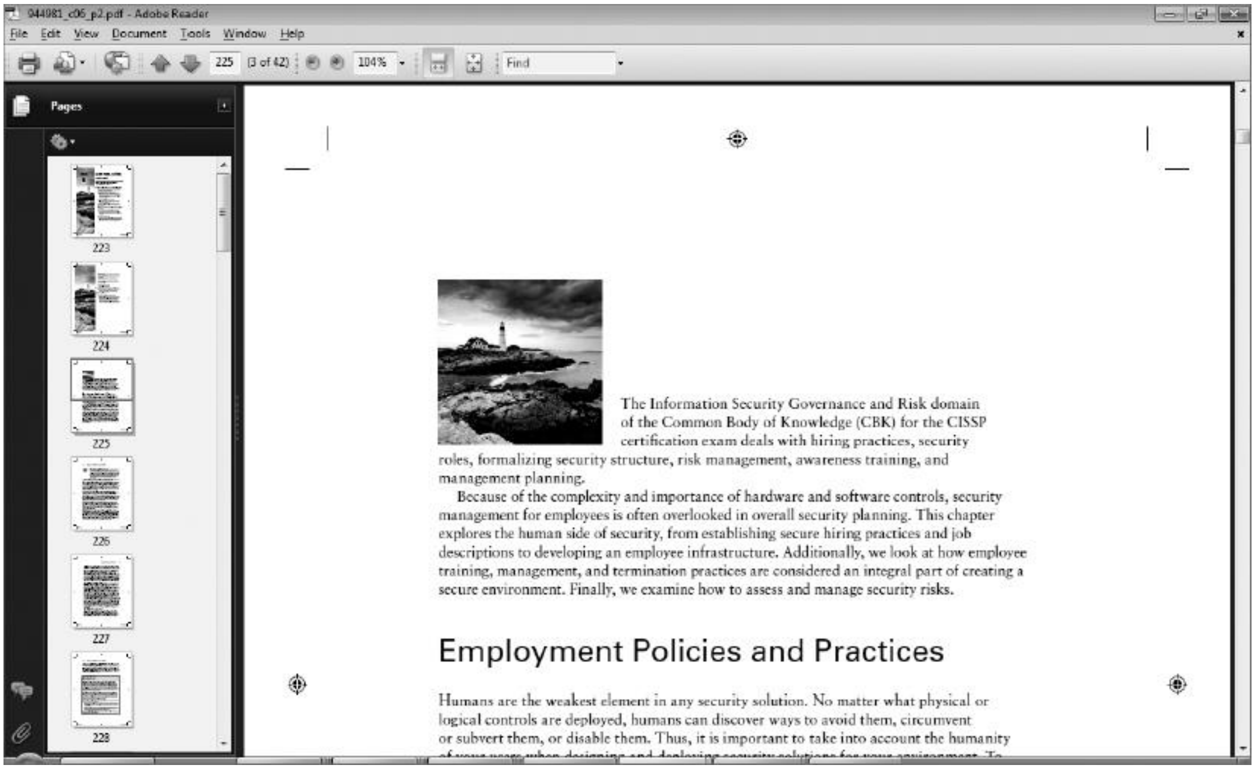
○ C. Encryption

○ D. Layering

Your Answer:

Search through the complete book in PDF!

- Access the entire *CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition* complete with figures and tables, in electronic format.
- Search the *CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition*chapters to find information on any topic in seconds.
- Also included in PDF format is a Glossary of key references.



The Information Security Governance and Risk domain of the Common Body of Knowledge (CBK) for the CISSP certification exam deals with hiring practices, security roles, formalizing security structure, risk management, awareness training, and management planning.

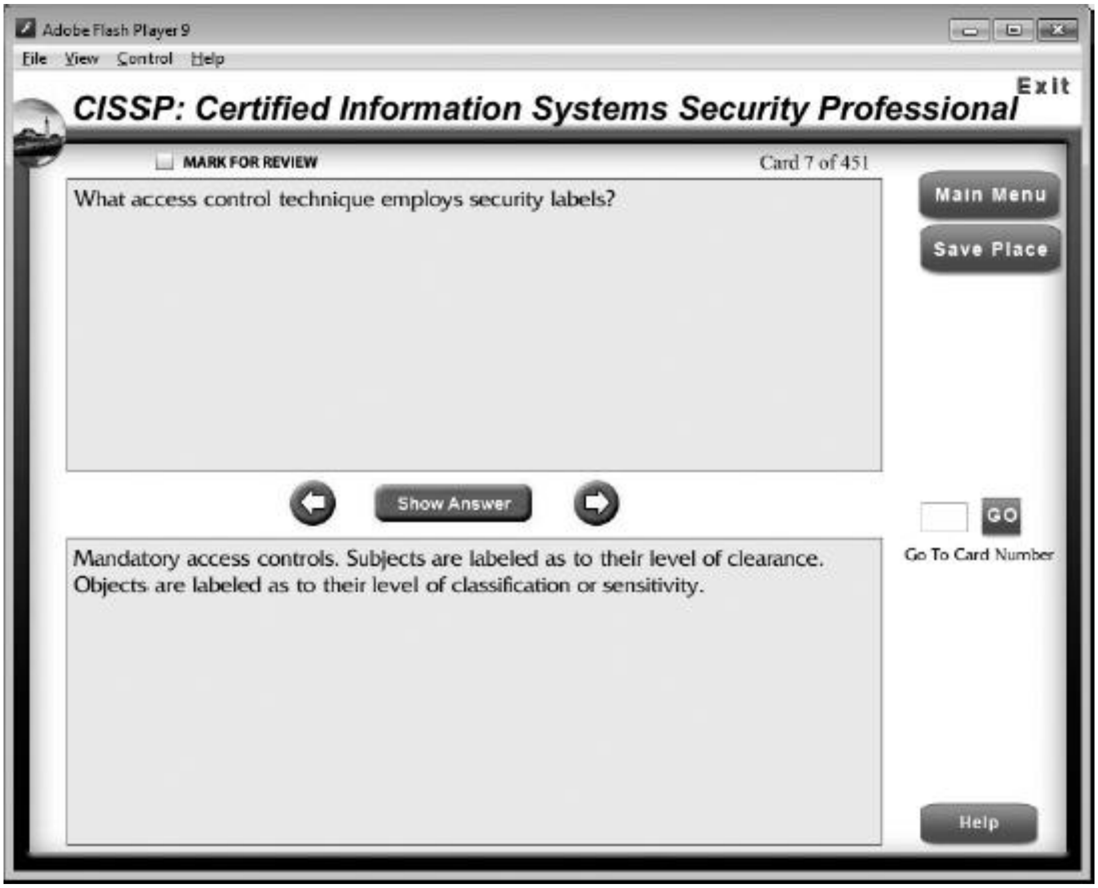
Because of the complexity and importance of hardware and software controls, security management for employees is often overlooked in overall security planning. This chapter explores the human side of security, from establishing secure hiring practices and job descriptions to developing an employee infrastructure. Additionally, we look at how employee training, management, and termination practices are considered an integral part of creating a secure environment. Finally, we examine how to assess and manage security risks.

Employment Policies and Practices

Humans are the weakest element in any security solution. No matter what physical or logical controls are deployed, humans can discover ways to avoid them, circumvent or subvert them, or disable them. Thus, it is important to take into account the humanity

Use the Electronic Flashcards to jog your memory and prep last minute for the exam!

- Reinforce your understanding of key concepts with these hardcore flashcard-style questions.
- Now you can study for the CISSP exam any time, anywhere.



What access control technique employs security labels?

Mandatory access controls. Subjects are labeled as to their level of clearance. Objects are labeled as to their level of classification or sensitivity.

CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition

CISSP Common Body of Knowledge

KEY AREA OF KNOWLEDGE	CHAPTER
ACCESS CONTROL	
Control access by applying the following concepts/methodology/techniques: Policies; types of controls (preventative, detective, corrective, etc.); techniques (e.g., non-discretionary, discretionary and mandatory); Identification and Authentication; Decentralized/distributed access control techniques; Authorization mechanisms; Logging and Monitoring	1, 2, 14

Understand access control attacks	2
Assess effectiveness of access controls	2
APPLICATION DEVELOPMENT SECURITY	
Understand and apply security in the system life cycle Systems Development Life Cycle (SDLC); Maturity models; Operation and maintenance; Change management; Perform risk analysis	7
Understand the application environment and security controls Security of the application environment; Security issues of programming languages; Security issues in source code (eg., buffer overflow); Configuration management	7, 8
Assess the effectiveness of application security Certification and accreditation; Auditing and logging; Corrective actions	7
BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING	
Understand business continuity requirements Develop and document project scope and plan	15, 16
Conduct business impact analysis Identify and prioritize critical business functions; Determine maximum tolerable downtime and other criteria; assess exposure to outages (e.g., local, regional, global); Define recovery objectives	15, 16
Develop recovery strategy Implement a backup storage strategy (e.g., offsite storage, electronic vaulting, tape rotation); recovery site strategies	15, 16

Understand disaster recovery process Response; Personnel; Communications; Assessment; Restoration	16
Provide Training	16
Test, update, assess and maintain the plan (e.g., version control, distribution)	16
CRYPTOGRAPHY	
Understand the application and use of cryptography Data at rest (e.g., Hard Drive); Data in transit (e.g., “On the wire”)	9, 10
Understand encryption concepts Foundational concepts; Symmetric cryptography; Asymmetric cryptography; Hybrid cryptography; Message digests; Hashing	9, 10
Understand key management process Creation/distribution; Storage/destruction; Recovery; Key escrow	10
Understand digital signatures	10
Understand methods of cryptanalytic attacks Chosen plain-text; Social engineering for key discovery; Brute Force; Cipher-text only; Known plaintext; Frequency analysis; Chosen cipher-text; implementation attacks	10
Employ cryptography in network security	10
Use cryptography to maintain e-mail security	10
Understand Public Key Infrastructure (PKI)	10

Understand certificate related issues	10
Understand information hiding alternatives (e.g., steganography, watermarking)	10
INFORMATION SECURITY GOVERNANCE AND RISK MANAGEMENT	
Understand and align security function to goals, mission, and objectives of the organization)	6
Understand and apply security governance Organizational processes; define security roles and responsibilities; Legislative and regulatory compliance; Privacy requirements compliance; Control frameworks; Due care; Due diligence	5, 6
Understand and apply concepts of confidentiality, availability, and integrity	5
Develop and implement security policy Security policies; Standards/baselines; Procedures; Guidelines; Documentation	6
Define and implement information classification and ownership	5, 6
Ensure security in contractual agreements and procurement processes	6
Understand and apply risk management concepts Identify threats and vulnerabilities; Risk assessment/analysis; risk assignment/acceptance; Countermeasure selection	5, 6
Evaluate personnel security Background checks and employment candidate screening; Employment agreements and policies; Employee termination processes; Vendor, consultant and contractor controls	5, 6

Develop and manage security education, training, and awareness	6
Develop and implement information system security strategies	5, 6
Support certification and accreditation efforts	5, 6, 12
Assess the completeness and effectiveness of the security program	5, 6, 12
Understand professional ethics	18
(ISC)^2 code of professional ethics; Support organization’s code of ethics	
Manage the Security Function Budget; Metrics; Resources	6
LEGAL, REGULATIONS, INVESTIGATIONS AND COMPLIANCE	
Understand legal issues that pertain to information security internationally Computer crime; Licensing and intellectual property (e.g., copyright, trademark); Import/Export; Trans-border data flow; Privacy	17, 18
Understand and support investigations Policy; Incident handling and response; Evidence collection and handling (e.g., chain of custody, interviewing); Reporting and documenting	14, 17, 18
Understand forensic procedures Media analysis; Network analysis; Software analysis	17, 18
Understand compliance requirements and procedures Regulatory environment; Audits; Reporting	6, 14,

	17, 18
OPERATIONS SECURITY	
Understand the following security concepts Need-to-know/least privilege; Separation of duties and responsibilities; Monitor special privileges (e.g., operators, administrators); Job rotation; Marking, handling, storing, and destroying of sensitive information and media; Record retention	13, 14, 6
Employ resource protection Media management; Asset management; Personnel privacy and safety	13, 14
Manage incident response Detection; Response; Reporting; Recovery; Remediation	18, 14, 15, 16, 17, 19
Prevent or respond to attacks (e.g., malicious code, zero-day exploit, denial of service)	8, 14
Implement and support patch and vulnerability management	2, 8
Understand configuration management concepts (e.g., versioning, baselining)	13, 7
Understand fault tolerance requirements	2, 15, 4
PHYSICAL (ENVIRONMENTAL) SECURITY	
Participate in site and facility design considerations	19

Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)	19
Support the implementation and operation of interior security (e.g., escort requirements/visitor control, keys and locks)	19
Support the implementation and operation of operations or facility security Communications and server rooms; Restricted and work area security; Data center security; Utilities and HVAC considerations; Water issues (e.g., leakage, flooding); Fire prevention, detection and suppression	19
Support the protection and securing of equipment	19
SECURITY ARCHITECTURE AND DESIGN	
Understand the fundamental concepts of security models (e.g., Confidentiality; Integrity; and Multi-level Models	11, 12
Understand the components of information systems security evaluation models Product evaluation models (e.g., common criteria); Industry and international security implementation guidelines (e.g., PCI-DSS, ISO)	12
Understand security capabilities of information systems (e.g., memory protection; virtualization, trusted platform module)	11, 12
Understand the vulnerabilities of security architecture System (e.g., covert channels; states attacks; emanations); Technology and process integration (e.g., single point of failure, service oriented architecture)	11, 12
Understand application and system vulnerabilities and threats Web-based (e.g., XML, SAML); Client-based (e.g., applets); Server-based (e.g., data flow control); Database security (e.g., inference, aggregation, data mining)	11, 12
Understand countermeasure principles (e.g., defense in depth)	12, 1

TELECOMMUNICATIONS AND NETWORK SECURITY	
Establish secure data communications	3, 4
Understand secure network architecture and design OSI and TCP/IP models; IP networking	3
Secure network components Hardware (e.g., modems, switches; routers); Transmission media; Filtering devices (e.g., firewalls, proxies); end-point security	3, 4
Establish secure multimedia communications Voice over IP (VoIP); Multimedia collaboration (e.g., remote meeting technology, instant messaging); Virtual Private Networks (VPN); Remote access	3, 4
Understand network attacks	4

The (ISC)^2 BOK is subject to change at any time without prior notice and at (ISC)^2's sole discretion. Please visit (ISC)^2's website (https://www.isc2.org/) for the most up-to-date information.

Glossary

Numbers and Symbols

** (star) Integrity Axiom (* Axiom)*

An axiom of the Biba model that states that a subject at a specific classification level cannot write data to a higher classification level. This is often shortened to “no write up.”

** (star) Security Property (* Property)*

A property of the Bell-LaPadula model that states that a subject at a specific classification level cannot write data to a lower classification level. This is often shortened to “no write down.”

802.11i (WPA-2)

An amendment to the 802.11 standard that defines a new authentication and encryption technique that is similar to IPSec. To date, no real-world attack has compromised a properly configured WPA-2 wireless network.

802.1x

A form of wireless authentication protection that requires all wireless clients to pass a gauntlet of RADIUS or TACACS services before network access is granted.

1000Base-T

A form of twisted-pair cable that supports 1000Mbps or 1Gbs throughput at 100 meter distances. Often called Gigabit Ethernet.

100Base-TX

Another form of twisted-pair cable similar to 100Base-T.

10Base2

A type of coaxial cable. Often used to connect systems to backbone trunks. 10Base2 has a maximum span of 185 meters with maximum throughput of 10Mpbs. Also called thinnet.

10Base5

A type of coaxial cable. Often used as a network’s backbone. 10Base5 has a maximum span of 500 meters with maximum throughput of 10Mpbs. Also called thicknet.

10Base-T

A type of network cable that consists of four pairs of wires that are twisted around each other and then sheathed in a PVC insulator. Also called twisted-pair.

A

abnormal activity

Any system activity that does not normally occur on your system. Also referred to as suspicious activity.

abstraction

The collection of similar elements into groups, classes, or roles for the assignment of security controls, restrictions, or permissions as a collective.

acceptance testing

A form of testing that attempts to verify that a system satisfies the stated criteria for functionality and possibly also for security capabilities of a product. It is used to determine whether end users or customers will accept the completed product.

accepting risk

The valuation by management of the cost/benefit analysis of possible safeguards and the determination that the cost of the countermeasure greatly outweighs the possible cost of loss because of a risk.

access

The transfer of information from an object to a subject.

access control

The mechanism by which subjects are granted or restricted access to objects.

access control list (ACL)

The column of an access control matrix that specifies what level of access each subject has over an object.

access control matrix

A table of subjects and objects that indicates the actions or functions that each subject can perform on each object. Each column of the matrix is an ACL. Each row of the matrix is a capability list.

access tracking

Auditing, logging, and monitoring the attempted access or activities of a subject. Also referred to as activity tracking.

account lockout

An element of the password policy's programmatic controls that disables a user account after a specified number of failed logon attempts. Account lockout is an effective countermeasure to brute-force and dictionary attacks against a system's logon prompt.

accountability

The process of holding someone responsible (accountable) for something. In this context, accountability is possible if a subject's identity and actions can be tracked and verified.

accreditation

The formal declaration by the Designated Approving Authority (DAA) that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

ACID model

The letters in ACID represent the four required characteristics of database transactions: atomicity, consistency, isolation, and durability.

active content

Web programs that users download to their own computer for execution rather than consuming server-side resources.

ActiveX

Microsoft's component object model (COM) technology used in web applications. ActiveX is implemented using any one of a variety of languages, including Visual Basic, C, C++, and Java.

Address Resolution Protocol (ARP)

A subprotocol of the TCP/IP protocol suite that operates at the Data Link layer (layer 2). ARP is used to discover the MAC address of a system by polling using its IP address.

addressing

The means by which a processor refers to various locations in memory.

administrative access controls

The policies and procedures defined by an organization's security policy to implement and enforce overall access control. Examples of administrative access controls include hiring practices, background checks, data classification, security training, vacation history reviews, work supervision, personnel controls, and testing.

administrative law

Regulations that cover a range of topics from procedures to be used within a federal agency to immigration policies that will be used to enforce the laws passed by Congress. Administrative law is published in the Code of Federal Regulations (CFR).

administrative physical security controls

Security controls that include facility construction and selection, site management, personnel controls, awareness training, and emergency response and procedures.

admissible evidence

Evidence that is relevant to determining a fact. The fact that the evidence seeks to determine must be material (in other words, related) to the case. In addition, the evidence must be competent, meaning that it must have been obtained legally. Evidence that results from an illegal search would be inadmissible because it is not competent.

Advanced Encryption Standard (AES)

The encryption standard selected in October 2000 by the National Institute for Standards and Technology (NIST) that is based on the Rijndael cipher.

advisory policy

A policy that discusses behaviors and activities that are acceptable and defines consequences of violations. An advisory policy discusses the senior management's desires for security and compliance within an organization. Most policies are advisory.

agent

Intelligent code objects that perform actions on behalf of a user. They typically take initial instructions from the user and then carry on their activity in an unattended manner for a predetermined period of time, until certain conditions are met, or for an indefinite period.

aggregate functions

SQL functions, such as `COUNT()`, `MIN()`, `MAX()`, `SUM()`, and `AVG()`, that can be run against a database to produce an information set.

aggregation

A number of functions that combine records from one or more tables to produce potentially useful information.

Agile Software Development

A set of software development approaches that eschew the rigid models of the past in favor of approaches that place an emphasis on the needs of the customer, and on quickly developing new functionality that meets those needs in an iterative fashion.

alarm

A mechanism that is separate from a motion detector and triggers a deterrent, triggers a repellant, and/or triggers a notification. Whenever a motion detector registers a significant or meaningful change in the environment, it triggers an alarm.

alarm triggers

Notifications sent to administrators when a specific event occurs.

amplifier

See *repeater*.

AND

The operation (represented by the ∧ symbol) that checks to see whether two values are both true.

analytic attack

An algebraic manipulation that attempts to reduce the complexity of a cryptographic algorithm. This attack focuses on the logic of the algorithm itself.

annualized loss expectancy (ALE)

The possible yearly cost of all instances of a specific realized threat against a specific asset. The ALE is calculated using the formula ALE = single loss expectancy (SLE) * annualized rate of occurrence (ARO).

annualized rate of occurrence (ARO)

The expected frequency that a specific threat or risk will occur (in other words, become realized) within a single year.

anomaly detection

See *behavior-based detection*.

APIPA

See *automatic private IP addressing (APIPA)*.

applet

Code objects sent from a server to a client to perform some action. Applets are self-contained miniature programs that execute independently of the server that sent them.

Application layer

Layer 7 of the Open Systems Interconnection (OSI) model.

application-level gateway firewall

A firewall that filters traffic based on the Internet service (in other words, application) used to transmit or receive the data. Application-level gateways are known as second-generation firewalls.

assembly language

A higher-level alternative to machine language code. Assembly languages use mnemonics to represent the basic instruction set of a CPU but still require hardware-specific knowledge.

asset

Anything within an environment that should be protected. The loss or disclosure of an asset could result in an overall security compromise, loss of productivity, reduction in profits, additional expenditures, discontinuation of the organization, and numerous intangible consequences.

asset valuation

A dollar value assigned to an asset based on actual cost and nonmonetary expenses, such as costs to develop, maintain, administer, advertise, support, repair, and replace; as well as other values, such as public confidence, industry support, productivity enhancement, knowledge equity, and ownership benefits.

asset value (AV)

A dollar value assigned to an asset based on actual cost and nonmonetary expenses.

assigning risk

See *transferring risk*.

assurance

The degree of confidence that security needs are satisfied. Assurance must be continually maintained, updated, and reverified.

asymmetric key

Public key cryptosystems that use a pair of keys (public and private) for each participant. Messages encrypted with one key from the pair can only be decrypted with the other key from the same pair.

asynchronous transfer mode (ATM)

A cell-switching technology rather than a packet-switching technology like Frame Relay. ATM uses virtual circuits much like Frame Relay, but because it uses fixed-size frames or cells, it can guarantee throughput. This makes ATM an excellent WAN technology for voice and video conferencing.

atomicity

One of the four required characteristics of all database transactions. A database transaction must be an "all-or-nothing" affair. If any part of the transaction fails, the entire transaction must be rolled back as if it never occurred.

attack

The exploitation of a vulnerability by a threat agent.

attacker

Any person who attempts to perform a malicious action against a system.

attenuation

The loss of signal strength and integrity on a cable because of the length of the cable.

attribute

A column within a table of a relational database.

audit trails

The records created by recording information about events and occurrences into a database or log file. Audit trails are used to reconstruct an event, to extract information about an incident, to prove or disprove culpability, and much more.

auditing

A methodical examination or review of an environment to ensure compliance with regulations and to detect abnormalities, unauthorized occurrences, or outright crimes.

auditor

The person or group responsible for testing and verifying that the security policy is properly implemented and the derived security solutions are adequate.

authentication

The process of verifying or testing that the identity claimed by a subject is valid.

Authentication Header (AH)

An IPSec protocol that provides authentication, integrity, and nonrepudiation.

authentication protocols

Protocol used to provide the transport mechanism for logon credentials.

Authentication Service (AS)

An element of the Kerberos Key Distribution Center (KDC). The AS verifies or rejects the authenticity and timeliness of tickets.

authorization

A process that ensures that the requested activity or object access is possible given the rights and privileges assigned to the authenticated identity (in other words, subject).

automatic private IP addressing (APIPA)

A feature of Windows that assigns an IP address to a system should DHCP address assignment fail. The IP address range used by APIPA is 169.254.0.0 - 169.254.255.255.

auxiliary alarm system

An additional function that can be added to either local or centralized alarm systems. The purpose of an auxiliary alarm system is to notify local police or fire services when an alarm is triggered.

availability

The assurance that authorized subjects are granted timely and uninterrupted access to objects.

awareness

A form of security teaching that is a prerequisite to training. The goal of awareness is to bring security into the forefront and make it a recognized entity for students/users.

B

badges

Forms of physical identification and/or of electronic access control devices.

Base+Offset addressing

An addressing scheme that uses a value stored in one of the CPU's registers as the base location from which to begin counting. The CPU then adds the offset supplied with the instruction to that base address and retrieves the operand from the computed memory location.

baseband

A communication medium that supports only a single communication signal at a time.

baseline

The minimum level of security that every system throughout the organization must meet. A baseline can be more than a security baseline. It can also be a performance baseline (used by behavior-based IDSs), or a configuration baseline (used for configuration management).

Basic Input/Output System (BIOS)

The operating system–independent primitive instructions that a computer needs to start up and load the operating system from disk.

Basic Rate Interface (BRI)

An ISDN service type that provides two B, or data, channels and one D, or management, channel. Each B channel offers 64Kbps, and the D channel offers 16Kbps.

behavior

In the context of object-oriented programming terminology and techniques, the results or output from an object after processing a message using a method.

behavior-based detection

An intrusion discovery mechanism used by IDS. Behavior-based detection finds out about the normal activities and events on your system through watching and learning. Once it has accumulated enough data about normal activity, it can detect abnormal and possible malicious activities and events. Also known as statistical intrusion detection, anomaly detection, and heuristics-based detection.

Bell-LaPadula model

A confidentiality-focused security model based on the state machine model and employing mandatory access controls and the lattice model.

best evidence rule

A rule that states that when a document is used as evidence in a court proceeding, the original document must be introduced. Copies will not be accepted as evidence unless certain exceptions to the rule apply.

Biba model

An integrity-focused security model based on the state machine model and employing mandatory access controls and the lattice model.

bind variable

A placeholder for SQL literal values, such as numbers or character strings.

biometrics

The use of human physiological or behavioral characteristics as authentication factors for logical access and identification for physical access.

birthday attack

An attack in which the malicious individual seeks to substitute in a digitally signed communication with a different message that produces the same message digest, thereby maintaining the validity of the original digital signature. This is based on the statistical anomaly that in a room with 23 people, the probability of two of more people having the same birthday is greater than 50 percent.

black-box testing

A form of program testing that examines the input and output of a program without focusing on its internal logical structures.

blackout

A complete loss of power.

block cipher

A cipher that applies the encryption algorithm to an entire message block at the same time. Transposition ciphers are examples of block ciphers.

Blowfish

A block cipher that operates on 64-bit blocks of text and uses variable-length keys ranging from a relatively insecure 32 bits to an extremely strong 448 bits.

bluejacking

Hijacking a Bluetooth connection to eavesdrop or extract information from devices.

Bluetooth (802.15)

A wireless standard commonly used to pair accessories to cell phones or computers.

boot sector

The portion of a storage device used to load the operating system and the types of viruses that attack that process.

bot

An intelligent agent that continuously crawls a variety of websites retrieving and processing data on behalf of the user.

bounds

The limits to the memory and resources a process can access.

breach

The occurrence of a security mechanism being bypassed or thwarted by a threat agent.

bridge

A network device used to connect networks with different speeds, cable types, or topologies that still use the same protocol. A bridge is a layer 2 device.

broadband

A communication medium that supports multiple communication signals simultaneously.

broadcast

A communications transmission to multiple but unidentified recipients.

broadcast address

A broadcast network address that is used during a smurf attack.

brouter

A network device that first attempts to route and then defaults to bridging if routing fails.

brownout

A period of prolonged low voltage.

brute force

An attack pattern characterized by a mechanical series of sequential or combinatorial inputs utilized in an automated attempt to identify security properties (usually passwords) in a given system (see brute-force attack).

brute-force attack

An attack made against a system to discover the password to a known identity (in other words, username). A brute-force attack uses a systematic trial of all possible character combinations to discover an account's password.

buffer overflow

A vulnerability that can cause a system to crash or allow the user to execute shell commands and gain access to the system. Buffer overflow vulnerabilities are especially prevalent in code developed rapidly for the Web using CGI or other languages that allow unskilled programmers to quickly create interactive web pages.

business attack

An attack that focuses on illegally obtaining an organization's confidential information.

Business Continuity Planning (BCP)

The assessment of a variety of risks to organizational processes and the creation of policies, plans, and procedures to minimize the impact those risks might have on the organization if they were to occur.

Business Impact Analysis (BIA)

See Business Impact Assessment (BIA).

Business Impact Assessment (BIA)

An analysis that identifies the resources that are critical to an organization's ongoing viability and the threats posed to those resources. It also assesses the likelihood that each threat will actually occur and the impact those occurrences will have on the business. a.k.a. Business Impact Analysis (BIA)

C

cache RAM

A process by that takes data from slower devices and temporarily stores it in higher-performance devices when its repeated use is expected.

campus area network (CAN)

A network that spans a college, university, or a multibuilding office complex.

capability list

Each row of an access control matrix is a capability list. A capability list is tied to the subject; it lists valid actions that can be taken on each object.

cardinality

The number of rows in a relational database.

cell suppression

The act of suppressing (or hiding) individual data items inside a database to prevent aggregation or inference attacks.

centralized access control

Method of control in which all authorization verification is performed by a single entity within a system.

centralized alarm system

An alarm system that signals a remote or centralized monitoring station when the alarm is triggered.

certificate authority

An agency that authenticates and distributes digital certificates.

certificate revocation list (CRL)

The list of certificates that have been revoked by a certificate authority before the lifetimes of the certificates have expired.

certificates

Endorsed copies of an individual’s public key that verifies their identity.

certification

The comprehensive evaluation, made in support of the accreditation process, of the technical and nontechnical security features of an IT system and other safeguards to establish the extent to which a particular design and implementation meets a set of specified security requirements.

chain of evidence

The process by which an object is uniquely identified in a court of law.

Challenge Handshake Authentication Protocol (CHAP)

One of the authentication protocols used over PPP links. CHAP encrypts usernames and passwords.

change management

The means by which changes to an environment are logged and monitored in order to ensure that any change does not lead to reduced or compromised security.

checklist test

A process in which copies of the disaster recovery checklists are distributed to the members of the disaster recovery team for their review.

Children's Online Privacy Protection Act (COPPA)

A law in the United States that places specific demands upon websites that cater to children or knowingly collect information from children.

chosen cipher-text attack

An attack in which the attacker has the ability to decrypt chosen portions of the cipher-text message.

chosen plain-text attack

An attack in which the attacker has the ability to encrypt plaintext messages of their choosing and then analyze the cipher-text output of the encryption algorithm.

CIA Triad

The three essential security principles of confidentiality, integrity, and availability.

cipher

A system that hides the true meaning of a message. Ciphers use a variety of techniques to alter and/or rearrange the characters or words of a message to achieve confidentiality.

Cipher Block Chaining (CBC)

A process in which each block of unencrypted text is XORed with the block of cipher text immediately preceding it before it is encrypted using the DES algorithm.

Cipher Feedback (CFB)

A mode in which the DES algorithm is used to encrypt the preceding block of cipher text. This block is then XORed with the next block of plain text to produce the next block of cipher text.

cipher text

A message that has been encrypted for transmission.

civil laws

Laws that form the bulk of the body of laws in the United States. They are designed to provide for an orderly society and govern matters that are not crimes but require an impartial arbiter to settle disputes between individuals and organizations.

Clark-Wilson model

A model that employs limited interfaces or programs to control and maintain object integrity.

class

In the context of object-oriented programming terminology and techniques, a collection of common methods from a set of objects that defines the behavior of those objects.

classification

A label that is applied to a resource to indicate its sensitivity or value to an organization and therefore designate the level of security necessary to protect that resource.

classification level

Another term for a security label. An assigned importance or value placed on objects and subjects.

clean power

Nonfluctuating pure power.

clearing

A method of sufficiently deleting media that will be reused in the same secured environment. Also known as overwriting.

click-wrap license agreement

A software agreement in which the contract terms are either written on the software box or included in the software documentation. During the installation process, you are required to click a button indicating that you have read the terms of the agreement and agree to abide by them.

clipping level

A threshold value used in violation analysis auditing. Crossing the clipping level triggers the recording of relevant event data to an audit log.

closed-circuit television (CCTV)

A security system using video cameras and video recording devices.

closed head system

See *wet pipe system*.

clustering (or key clustering)

A weakness in cryptography where a plain-text message generates identical cipher-text messages using the same algorithm but using different keys.

coaxial cable

A cable with a center core of copper wire surrounded by a layer of insulation and then by a conductive braided shielding and finally encased in an insulation sheath. Coaxial cable is fairly resistant to EMI, has a low cost, and is easy to install.

Control Objectives for Information and related Technology (CobiT)

A security concept infrastructure used to organize the complex security solution of companies.

code

See *cipher*.

cohesive (or cohesiveness)

An object is highly cohesive if it can perform a task with little or no help from other objects. Highly cohesive objects are not as dependent upon other objects as objects with lower cohesion. Objects with higher cohesion are often better. Highly cohesive objects perform tasks alone and have low coupling.

cognitive password

A variant of the password authentication factor that asks a series of questions about facts or predefined responses that only the subject should know.

cold sites

Standby facilities large enough to handle the processing load of an organization and with appropriate electrical and environmental support systems.

collision attack

See *birthday attack*.

collusion

An agreement between multiple people to perform an unauthorized or illegal action.

commercial business/private sector classification

The security labels commonly employed on secure systems used by corporations. Common corporate or commercial security labels are confidential, proprietary, private, sensitive, and public.

Committed Information Rate (CIR)

A contracted minimum guaranteed bandwidth allocation for a virtual circuit.

Common Body of Knowledge (CBK)

The areas of information prescribed by (ISC)^2 as the source of knowledge for the CISSP exam.

common mode noise

Electromagnetic interference (EMI) noise generated by the difference in power between the hot and ground wires of a power source or operating electrical equipment.

Common Object Request Broker Architecture (CORBA)

An international standard for distributed computing. CORBA enables code operating on a computer to locate resources located elsewhere on the network.

companion virus

A variation of the file infector virus. A companion virus is a self-contained executable file that escapes detection by using a filename similar to, but slightly different from, a legitimate operating system file.

compartmented security mode

A security mode in which systems process two or more types of compartmented information. All system users must have an appropriate clearance to access all information processed by the system but do not necessarily need to know all the information in the system.

compensation access control

A type of access control that provides various options to other existing controls to aid in the enforcement and support of a security policy.

competent

A distinction of evidence that means that the evidence must be obtained legally. Evidence that results from an illegal search would be inadmissible because it is not competent.

compiled languages

A computer language that is converted into machine language before distribution or execution.

compliance testing

Another common usage of auditing. Verification that a system complies with laws, regulations, baselines, guidelines, standards, and policies is an important part of maintaining security in any environment.

Component Object Model (COM)

Microsoft’s standard for the use of components within a process or between processes running on the same system.

compromise

If system security has been broken, the system is considered compromised.

computer architecture

An engineering discipline concerned with the construction of computing systems from the logical level.

computer crime

Any crime that is perpetrated against or with the use of a computer.

Computer Fraud and Abuse Act

A U.S. law written to exclusively cover computer crimes that cross state boundaries to avoid infringing upon states' rights.

Computer Security Act (CSA) of 1987

A U.S. law that mandates baseline security requirements for all federal agencies.

concentrator

See *repeater*.

conclusive evidence

Incontrovertible evidence that overrides all other forms of evidence.

concurrency

A security mechanism that endeavors to make certain that the information stored in a database is always correct or at least has its integrity and availability protected. Concurrency uses a "lock" feature to allow an authorized user to make changes and then "unlocks" data elements only after all changes are complete.

Confidential

A government/military classification used for data of a confidential nature. Unauthorized disclosure of confidential data will have noticeable effects and cause damage to national security. This classification is used for all data between secret and sensitive but unclassified classifications.

confidentiality

The assurance that information is protected from unauthorized disclosure and the defined level of secrecy is maintained throughout all subject-object interactions.

configuration management

The process of logging, auditing, and monitoring activities related to security controls and security mechanisms over time. This data is then used to identify agents of change, whether objects, subjects, programs, communication pathways, or even the network itself.

confinement (or confinement property)

The principle that allows a process to read from and write to certain memory locations and resources only. This is an alternate name for the * (star) Security Property of the Bell-LaPadula model.

confusion

It occurs when the relationship between the plain text and the key is complicated enough that an attacker can't just alter the plain text and analyze the result in order to determine the key.

consistency

One of the four required characteristics of all database transactions (the other three are atomicity, isolation, and durability). All transactions must begin operating in an environment that is consistent with all of the database's rules.

contamination

The result of mixing of data with a different classification level and/or need-to-know requirement.

content-dependent access control

A form of access control based on the contents or payload of an object.

context-dependent access control

A form of access control based on the context or surroundings of an object.

continuity

A goal an organization can accomplish by having plans and procedures to help mitigate the effects a disaster has on its continuing operations and to speed the return to normal operations.

contractual license agreement

A written contract between the software vendor and the customer outlining the responsibilities of each.

control

The use of access rules or countermeasures to limit a subject's access to an object.

controls gap

The difference between total risk and residual risk.

Copper Distributed Data Interface (CDDI)

Deployment of FDDI using twisted-pair (in other words, copper) wires. This reduces the maximum segment length to 100 meters and is susceptible to interference.

copyright

Law that guarantees the creators of "original works of authorship" protection against the unauthorized duplication of their work.

corrective access control

An access control deployed to restore systems to normal after an unwanted or unauthorized activity has occurred. Examples of corrective access controls include alarms, mantraps, and security policies.

corrective controls

Instructions, procedures, or guidelines used to reverse the effects of an unwanted activity, such as attacks or errors.

countermeasures

Actions taken to patch a vulnerability or secure a system against an attack. Countermeasures can include altering access controls, reconfiguring security settings, installing new security devices or mechanisms, adding or removing services, and so on.

coupling

The level of interaction between objects. Lower coupling means less interaction. Lower coupling delivers better software design because objects are more independent. Lower coupling is easier to troubleshoot and update. Objects with low cohesion require lots of assistance from other objects to perform tasks and have high coupling.

covert channel

The means by which data can be communicated outside of normal, expected, or detectable methods.

covert storage channel

A channel that conveys information by writing data to a common storage area where another process can read it.

covert timing channel

A channel that conveys information by altering the performance of a system component or modifying a resource's timing in a predictable manner.

cracker

Malicious users intent on waging an attack against a person or system. Crackers may be motivated by greed, power, or recognition. Their actions can result in stolen property (data, ideas, and so on), disabled systems, compromised security, negative public opinion, loss of market share, reduced profitability, and lost productivity.

creeping privilege(s)

When a user account accumulates privileges over time as job roles and assigned tasks change.

criminal law

Body of laws that the police and other law enforcement agencies enforce. Criminal law contains prohibitions against acts such as murder, assault, robbery, arson, theft, and similar offenses.

critical path analysis

A systematic effort to identify relationships between mission-critical applications, processes, and operations and all of the necessary supporting elements.

criticality prioritization

The prioritization of mission-critical assets and processes during the creation of BCP/DRP.

crossover error rate (CER)

The point at which the false acceptance rate (FAR) equals the false rejection rate (FRR). This is the point from which performance is measured in order to compare the capabilities of different biometric devices.

cryptanalysis

The study of methods to defeat codes and ciphers.

cryptographic key

Cryptographic keys provide the “secret” portion of a cryptographic algorithm used to encrypt and decrypt data.

cryptography

Algorithms applied to data that are designed to ensure confidentiality, integrity, authentication, and/or nonrepudiation.

cryptosystem

System in which a shared secret key or pairs of public and private keys are used by communicating parties to facilitate secure communication.

cryptovariable

Another name for the key used to perform encryption and decryption activities.

custodian

A subject that has been assigned or delegated the day-to-day responsibilities of classifying and labeling objects and properly storing and protecting objects. The custodian is typically the IT staff or the system security administrator.

cyclic redundancy check (CRC)

Similar to a hash total, a value that indicates whether a message has been altered or damaged in transit.

D

data circuit-terminating equipment (DCE)

A networking device that performs the actual transmission of data over the Frame Relay as well as establishing and maintaining the virtual circuit for the customer.

data classification

Grouping data under labels for the purpose of applying security controls and access restrictions.

data custodian

The user who is assigned the task of implementing the prescribed protection defined by the security policy and upper management. The data custodian performs any and all activities necessary to provide adequate protection for data and to fulfill the requirements and responsibilities delegated to him from upper management.

Data Definition Language (DDL)

The database programming language that allows for the creation and modification of the database's structure (known as the schema).

data dictionary

Central repository of data elements and their relationships. Stores critical information about data usage, relationships, sources, and formats.

data diddling

The act of making small changes to data.

Data Encryption Standard (DES)

A standard cryptosystem proposed in 1977 for all government communications. DES (and 3DES) was superseded by Advanced Encryption Standard (AES) in December 2001.

data extraction

The process of extracting elements of data from a large body of data to construct a meaningful representation or summary of the whole.

data hiding

The process of preventing data from being known by a subject.

Data Link layer

Layer 2 of the OSI model.

Data Manipulation Language (DML)

The database programming language that allows users to interact with the data contained within the schema.

data mart

The storage facility used to secure metadata.

data mining

A technique or tool that allows analysts to comb through data warehouses and look for potential correlated information amid the historical data.

data owner

The person responsible for classifying information for placement and protection within the security solution.

data steward

See data custodian

data terminal equipment (DTE)

A networking device that acts like a router or a switch and provides the customer's network access to the Frame Relay network.

data warehouse

Large databases used to store large amounts of information from a variety of databases for use in specialized analysis techniques.

database

An electronic filing system for organizing collections of information. Most databases are organized by files, records, and fields.

database management system (DBMS)

An application that enables the storage, modification, and extraction of information from a database.

database partitioning

The act of dividing a database up into smaller sections or individual databases; often employed to segregate content with varying sensitivity labels.

decentralized access control

System of access control in which authorization verification is performed by various entities located throughout a system.

decision support system (DSS)

An application that analyzes business data and presents it so as to make business decisions easier for users. DSS is considered an informational application more so than an operational application. Often a DSS is employed by knowledge workers (such as help desk or customer support) and by sales services (such as phone operators).

declassification

The process of moving a resource into a lower classification level once its value no longer justifies the security protections provided by a higher level of classification.

decrypt

The process of reversing a cryptographic algorithm that was used to encrypt a message.

dedicated mode

See *dedicated security mode*.

dedicated security mode

Mode in which the system is authorized to process only a specific classification level at a time. All system users must have clearance and a need to know that information.

deencapsulation

The process of stripping a layer's header and footer from a PDU as it travels up the OSI model layers.

degaussing

The act of using a magnet to return media to its original pristine unused state.

degree

The number of columns in a relational database.

delegation

In the context of object-oriented programming, the forwarding of a request by an object to another object or delegate. An object delegates if it does not have a method to handle the message.

delta rule

Also known as the learning rule. It is the feature of expert systems that allows them to learn from experience.

Delphi technique

An anonymous feedback and response process used to arrive at a group consensus.

deluge system

Another form of dry pipe (fire suppression) system that uses larger pipes and therefore a significantly larger volume of water. Deluge systems are inappropriate for environments that contain electronics and computers.

denial of service (DoS)

A type of attack that prevents a system from processing or responding to legitimate traffic or requests for resources and objects.

deny risk

See *reject risk*.

detective access control

An access control deployed to discover unwanted or unauthorized activity. Examples of detective access controls include security guards, supervising users, incident investigations, and intrusion detection systems (IDSs).

detective control

See *detective access control*.

deterrent access control

An access control that discourages violations of a security policy.

dictionary attack

An attack against a system designed to discover the password to a known identity (in other words, a username). In a dictionary attack, a script of common passwords and dictionary words is used to attempt to discover an account's password.

differential backup

A type of backup that stores all files that have been modified since the time of the most recent full backup.

Diffie-Hellman algorithm

A key exchange algorithm useful in situations in which two parties might need to communicate with each other but they have no physical means to exchange key material and there is no public key infrastructure in place to facilitate the exchange of secret keys.

diffusion

When a change in the plain-text results in multiple changes spread throughout the cipher text.

Digital Millennium Copyright Act

A law that establishes the prohibition of attempts to circumvent copyright protection mechanisms placed on a protected work by the copyright holder and limits the liability of Internet service providers when their circuits are used by criminals violating the copyright law.

digital signature

A method for ensuring a recipient that a message truly came from the claimed sender and that the message was not altered while in transit between the sender and recipient.

Digital Signature Standard (DSS)

A standard that specifies that all federally approved digital signature algorithms must use a secure hashing function.

direct addressing

A process by which the CPU is provided with the actual address of the memory location to be accessed.

direct evidence

Evidence that proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses.

Direct Sequence Spread Spectrum (DSSS)

A wireless technology that employs all of the available frequencies simultaneously in parallel.

directive access control

An access control that directs, confines, or controls the actions of subjects to force or encourage compliance with security policy.

detective control

Any security mechanism used to verify the effectiveness of directive and preventive controls.

directory service

A centralized database of resources available to the network, much like a telephone directory for network services and assets. Users, clients, and processes consult the directory service to learn where a desired system or resource resides.

Direct Memory Access (DMA)

A mechanism that allows devices to exchange data directly with real memory (RAM) without requiring assistance from the CPU.

disaster

An event that brings great damage, loss, or destruction to a system or environment.

disaster recovery plan

A document that guides the recovery efforts necessary to restore your business to normal operations as quickly as possible.

Disaster Recovery Planning (DRP)

Term that describes the actions an organization takes to resume normal operations after a disaster interrupts normal activity.

discretionary access control

A mechanism used to control access to objects. The owner or creator of an object controls and defines the access other subjects have to it.

Discretionary Security Property

Property that states that the system uses an access control matrix to enforce discretionary access control.

distributed access control

A form of access control in which authorization verification is performed by various entities located throughout a system.

Distributed Component Object Model (DCOM)

An extension of COM to support distributed computing. This is Microsoft's answer to CORBA.

distributed data model

In a distributed data model, data is stored in more than one database but remains logically connected. The user perceives the database as a single entity, even though it comprises numerous parts interconnected over a network. Each field may have numerous children as well as numerous parents. Thus, the data mapping relationship is many-to-many.

distributed denial of service (DDoS)

A distributed denial of service occurs when the attacker compromises several systems to be used as launching platforms against one or more victims. The compromised systems used in the attack are often called slaves or zombies. A DDoS attack results in the victims being flooded with data from numerous sources.

distributed reflective denial of service (DRDoS)

DRDoS attacks take advantage of the normal operation mechanisms of key Internet services, such as DNS and router update protocols. DRDoS attacks function by sending numerous update, session, or control packets to various Internet service servers or routers with a spoofed source address of the intended victim. A DRDoS attack can result in so much traffic that upstream systems are adversely affected by the sheer volume of data focused on the victim.

DNS poisoning

The act of altering or falsifying the information of DNS to route or misdirect legitimate traffic.

documentary evidence

Any written items brought into court to prove a fact at hand. This type of evidence must also be authenticated.

domain

1) A realm of trust or a collection of subjects and objects that share a common security policy. Each domain's access control is maintained independently of other domains' access control. This results in decentralized access control when multiple domains are involved. 2) An area of study for the CISSP exam.

dry pipe system

A fire suppression system that contains compressed air. Once suppression is triggered, the air escapes, which opens a water valve that in turn causes the pipes to fill and discharge water into the environment.

due care

The steps taken to ensure that assets and employees of an organization have been secured and protected and that upper management has properly evaluated and assumed all unmitigated or transferred risks.

due diligence

The extent to which a reasonable person will endeavor under specific circumstances to avoid harming other people or property.

dumb cards

Human-readable-only card IDs that usually have a photo and written information about the authorized bearer. Dumb cards are for use in environments where automated controls are infeasible or unavailable but security guards are practical.

dumpster diving

The act of digging through the refuse, remains, or leftovers from an organization or operation in order to discover or infer information about the organization.

durability

One of the four required characteristics of all database transactions (the other three are atomicity, consistency, and isolation). The concept that database transactions must be resilient. Once a transaction is committed to the database, it must be preserved. Databases ensure durability through the use of backup mechanisms, such as transaction logs.

dwell time

The length of time a key on the keyboard is pressed. This is an element of the keystroke dynamics biometric factor.

Dynamic Host Configuration Protocol (DHCP)

A protocol used to assign TCP/IP configuration settings to systems upon bootup. DHCP uses port 67 for server point-to-point response and port 68 for client request broadcast. DHCP supports centralized control and management of network addressing.

dynamic packet-filtering firewalls

A firewall that enables real-time modification of the filtering rules based on traffic content. Dynamic packet-filtering firewalls are known as fourth-generation firewalls.

dynamic passwords

Passwords that do not remain static for an extended period of time. Dynamic passwords can change on each use or at a regular interval, such as every 30 days.

E

eavesdropping

Another term for sniffing. However, eavesdropping can include more than just capturing and recording network traffic. Eavesdropping also includes recording or listening to audio communications, faxes, radio signals, and so on.

Economic Espionage Act of 1996

A law that states that anyone found guilty of stealing trade secrets from a U.S. corporation with the intention of benefiting a foreign government or agent may be fined up to $500,000 and imprisoned for up to 15 years and that anyone found guilty of stealing trade secrets under other circumstances may be fined up to $250,000 and imprisoned for up to 10 years.

education

A detailed endeavor where students/users learn much more than they actually need to know to perform their work tasks. Education is most often associated with users pursuing certification or seeking job promotion.

El Gamal

The explanation of how the mathematical principles behind the Diffie-Hellman key exchange algorithm could be extended to support an entire public key cryptosystem used for the encryption and decryption of messages.

electronic access control (EAC)

A type of smart lock that uses a credential reader, an electromagnet, and a door-closed sensor.

electronically erasable PROM (EEPROM)

A storage system that uses electric voltages delivered to the pins of the chip to force erasure. EEPROMs can be erased without removal from the computer, giving them much greater flexibility than standard PROM and EPROM chips.

electromagnetic interference (EMI)

A type of electrical noise that can do more than just cause problems with how equipment functions; it can also interfere with the quality of communications, transmissions, and playback.

Electronic Codebook (ECB)

The simplest encryption mode to understand and the least secure. Each time the algorithm processes a 64-bit block, it simply encrypts the block using the chosen secret key. This means that if the algorithm encounters the same block multiple times, it produces the same encrypted block.

Electronic Communications Privacy Act (ECPA)

The law that makes it a crime to invade an individual's electronic privacy. It protects against the monitoring of email and voice mail communications and prevents providers of those services from making unauthorized disclosures of their content.

electronic vaulting

A storage scenario in which database backups are transferred to a remote site in a bulk transfer fashion. The remote location may be a dedicated alternative recovery site (such as a hot site) or simply an offsite location managed within the company or by a contractor for the purpose of maintaining backup data.

elliptic curve cryptography

A new branch of public key cryptography that offers similar security to established public key cryptosystems at reduced key sizes.

elliptic curve group

Each elliptic curve has a corresponding elliptic curve group made up of the points on the elliptic curve along with the point O, located at infinity. Two points within the same elliptic curve group (P and Q) can be added together with an elliptic curve addition algorithm.

employee

Often referred to as the user when discussing IT issues. See also *user*.

employment agreement

A document that outlines an organization's rules and restrictions, security policy, and acceptable use and activities policies; details the job description;

outlines violations and consequences; and defines the length of time the position is to be filled by the employee.

Encapsulating Security Payload (ESP)

An element of IPSec that provides encryption to protect the confidentiality of transmitted data but can also perform limited authentication.

encapsulation

The process of adding a header and footer to a PDU as it travels down the OSI model layers.

encrypt

The process used to convert a message into cipher text.

encryption

The art and science of hiding the meaning or intent of a communication from recipients not meant to receive it.

end user

See *user*.

end-to-end encryption

An encryption algorithm that protects communications between two parties (in other words, a client and a server) and is performed independently of link encryption. An example of this would be the use of Privacy Enhanced Mail (PEM) to pass a message between a sender and a receiver. This protects against an intruder who might be monitoring traffic on the secure side of an encrypted link or traffic sent over an unencrypted link.

enrollment

The process of establishing a new user identity or authentication factor on a system. Secure enrollment requires physical proof of a person's identity or authentication factor. Generally, if the enrollment process takes longer than two minutes, the identification or authorization mechanism (typically a biometric device) is not approved.

entity

A subject or an object.

erasable PROM (EPROM)

A PROM chip that has a small window through which the illumination of a special ultraviolet light causes the contents of the chip to be erased. After this process is complete, the end user can burn new information into the EPROM.

erasing

A delete operation against a file, a selection of files, or the entire media. In most cases, the deletion or erasure process removes only the directory or catalog link to the data. The actual data remains on the drive.

Escrowed Encryption Standard

A failed government attempt to create a back door to all encryption solutions. The solution employed the Clipper chip, which used the Skipjack algorithm.

espionage

The malicious act of gathering proprietary, secret, private, sensitive, or confidential information about an organization for the express purpose of disclosing and often selling that data to a competitor or other interested organization (such as a foreign government).

Ethernet

A common shared media LAN technology.

ethical hackers

Those trained in responsible network security methodology, with a philosophy toward nondestructive and nonintrusive testing, ethical hackers attack security systems on behalf of their owners seeking to identify and document vulnerabilities so that they may be remediated before malicious hackers can exploit them. Ethical hackers use the same methods to test security that unethical ones do but report what they find rather than seeking to turn them to their advantage.

ethical hacking

See *penetration testing*.

ethics

The rules that govern personal conduct. Several organizations have recognized the need for standard ethics rules, or codes, and have devised guidelines for ethical behavior. These rules are not laws but are minimum standards for professional behavior. They should provide you with a basis for sound, professional, ethical judgment.

evidence

In the context of computer crime, any hardware, software, or data that you can use to prove the identity and actions of an attacker in a court of law.

excessive privilege(s)

More access, privilege, or permission than a user's assigned work tasks dictate. If a user account is discovered to have excessive privilege, the additional and unnecessary benefits should be immediately curtailed.

exit interview

An aspect of a termination policy. The terminated employee is reminded of their legal responsibilities to prevent the disclosure of confidential and sensitive information.

expert opinion

A type of evidence consisting of the opinions and facts offered by an expert. An expert is someone educated in a field and who currently works in that field.

expert system

A system that seeks to embody the accumulated knowledge of humankind on a particular subject and apply it in a consistent fashion to future decisions.

exposure

The condition of being exposed to asset loss because of a threat. Exposure involves being susceptible to the exploitation of a vulnerability by a threat agent or event.

exposure factor (EF)

The percentage of loss that an organization would experience if a specific asset were violated by a realized risk.

extranet

A cross between the Internet and an intranet. An extranet is a section of an organization's network that has been sectioned off so that it acts as an intranet for the private network but also serves information to a limited number of specific outsiders. Often access into an extranet from the Internet requires a VPN connection. Extranets are often used in B2B applications, between customers and suppliers.

F

face scan

An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. A face scan is a process by which the shape and feature layout of a person's face is used to establish identity or provide authentication.

fail-secure

See *fail-safe*.

fail-safe

The response of a system to a failure so that it defaults to a "deny" posture.

fail-open

The response of a system to a failure so that it defaults to an "allow" posture.

Fair Cryptosystems

A failed government attempt to create a back door to all encryption solutions. This technology used a segmented key that was divided among several trustees.

false acceptance rate (FAR)

Error that occurs when a biometric device is not sensitive enough and an invalid subject is authenticated. Also referred to as a Type 2 error.

false rejection rate (FRR)

Error that occurs when a biometric device is too sensitive and a valid subject is not authenticated. Also referred to as a Type 1 error.

Family Educational Rights and Privacy Act (FERPA)

A specialized privacy bill that affects any educational institution that accepts any form of funding from the federal government (the vast majority of schools). It grants certain privacy rights to students older than the age of 18 and the parents of minor students.

fault

A momentary loss of power.

Federal Information Processing Standard 140 (FIPS-140)

FIPS-140 defines the hardware and software requirements for cryptographic modules that the federal government uses.

Federal Sentencing Guidelines

A 1991 law that provides punishment guidelines for breaking federal laws.

fence

A perimeter-defining device. Fences are used to clearly differentiate between areas that are under a specific level of security protection and those that are not. Fencing can include a wide range of components, materials, and construction methods.

Fiber Distributed Data Interface (FDDI)

A high-speed token-passing technology that employs two rings with traffic flowing in opposite directions. FDDI offers transmission rates of 100Mbps and is often used as a backbone to large enterprise networks.

fiber-optic

A cabling form that transmits light instead of electrical signals. Fiber-optic cable supports throughputs up to 2 Gbps and lengths of up to 2 kilometers.

file infector

Virus that infects different types of executable files and triggers when the operating system attempts to execute them. For Windows-based systems, these files end with `.exe` and `.com` extensions.

financial attack

A crime that is carried out to unlawfully obtain money or services.

fingerprints

The patterns of ridges on the fingers of humans. Often used as a biometric authentication factor.

firewall

A network device used to filter traffic. A firewall is typically deployed between a private network and a link to the Internet, but it can be deployed between departments within an organization. Firewalls filter traffic based on a defined set of rules.

firmware

Software that is stored in a ROM chip.

flight time

The length of time between key presses. This is an element of the keystroke dynamics form of biometrics.

flooding

An attack that involves sending enough traffic to a victim to cause a DoS. Also referred to as a stream attack.

Fourth Amendment

An amendment to the U.S. Constitution that prohibits government agents from searching private property without a warrant and probable cause. The courts have expanded their interpretation of the Fourth Amendment to include protections against wiretapping and other invasions of privacy.

fraggle

A form of denial-of-service attack similar to smurf, but it uses UDP packets instead of ICMP.

fragment

When a network receives a packet larger than its maximum allowable packet size, it breaks it up into two or more fragments. These fragments are each assigned a size (corresponding to the length of the fragment) and an offset (corresponding to the starting location of the fragment).

fragmentation attacks

An attack that exploits vulnerabilities in the fragment reassembly functionality of the TCP/IP protocol stack.

Frame Relay

A shared connection medium that uses packet-switching technology to establish virtual circuits for customers.

frequency analysis

A cryptographic analysis or attack that looks for repetition of letters in an encrypted message and compares that with the statistics of letter usage for a specific language, such as the frequency of the letters *E*, *T*, *A*, *O*, *N*, *R*, *I*, *S*, and *H* in the English language.

Frequency Hopping Spread Spectrum (FHSS)

An early implementation of the spread spectrum concept. This wireless access technology transmits data in a series while constantly changing the frequency in use.

full backup

A complete copy of data contained on the protected device on the backup media. This also refers to the process of making a complete copy of data, as in "performing a full backup."

full-interruption tests

A disaster recovery test that involves actually shutting down operations at the primary site and shifting them to the recovery site.

full-knowledge teams

These possess a full body of knowledge over the operation, configuration, and utilization of hardware and software inventory prior to a security assessment or penetration test.

G

Gantt chart

A type of bar chart that shows the interrelationships over time between projects and schedules. It provides a graphical illustration of a schedule that helps to plan, coordinate, and track specific tasks in a project.

gate

A controlled exit and entry point in a fence.

gateway

A networking device that connects networks that are using different network protocols.

Government Information Security Reform Act of 2000

Act that amends the United States Code to implement additional information security policies and procedures.

government/military classification

The security labels commonly employed on secure systems used by the military. Military security labels range from highest sensitivity to lowest:

top secret, secret, confidential, sensitive but unclassified, and unclassified (top secret, secret, and confidential are collectively known as classified).

Gramm-Leach-Bliley (GLBA) Act

A law passed in 1999 that eased the strict governmental barriers between financial institutions. Banks, insurance companies, and credit providers were severely limited in the services they could provide and the information they could share with each other. GLBA somewhat relaxed the regulations concerning the services each organization could provide.

granular object control

A very specific and highly detailed level of control over the security settings of an object.

ground

The wire in an electrical circuit that is grounded (that is, connected with the earth).

group

An access control management simplification mechanism similar to a role. Similar users are made members of a group. A group is assigned access to an object. Thus, all members of the group are granted the same access to an object. The use of groups greatly simplifies the administrative overhead of managing user access to objects.

grudge attack

Attack usually motivated by a feeling of resentment and carried out to damage an organization or a person. The damage could be in the loss of information or harm to the organization or a person’s reputation. Often the attacker is a current or former employee or someone who wishes ill will upon an organization.

guideline

A document that offers recommendations on how standards and baselines are implemented. Guidelines outline methodologies, include suggested actions, and are not compulsory.

H

hacker

A technology enthusiast who does not have malicious intent. Many authors and the media often use the term when they are actually discussing issues relating to crackers.

Halon

A fire-suppressant material that converts to toxic gases at 900 degrees Fahrenheit and depletes the ozone layer of the atmosphere and is therefore usually replaced by an alternative material.

hand geometry

A type of biometric control that recognizes the physical dimensions of a hand. This includes width and length of the palm and fingers. It can be a mechanical or image-edge (in other words, visual silhouette) graphical solution.

handshaking

A three-way process utilized by the TCP/IP protocol stack to set up connections between two hosts.

hardware

An actual physical device, such as a hard drive, LAN card, printer, and so on.

hardware segmentation

A technique that implements process isolation at the hardware level by enforcing memory access constraints.

hash

A number known as a message digest generated from a hash function. Also see *hash function*.

hash function

The process of taking a full message and generating a unique output value derived from the content of the message. This value is commonly referred to as the message digest.

hash total

A checksum used to verify the integrity of a transmission. See also *cyclic redundancy check (CRC)*.

hash value

A number that is generated from a string of text and is substantially smaller than the text itself. A formula creates a hash value in a way that it is extremely unlikely that any other text will produce the same hash value.

Hashed Message Authentication Code (HMAC)

An algorithm that implements a partial digital signature—it guarantees the integrity of a message during transmission, but it does not provide for nonrepudiation.

Health Insurance Portability and Accountability Act (HIPAA)

A law passed in 1996 that made numerous changes to the laws governing health insurance and health maintenance organizations (HMOs). Among the provisions of HIPAA are privacy regulations requiring strict security measures for hospitals, physicians, insurance companies, and other organizations that process or store private medical information about individuals.

hearsay evidence

Evidence consisting of statements made to a witness by someone else outside of court. Computer log files that are not authenticated by a system administrator can also be considered hearsay evidence.

heart/pulse pattern

An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The heart/pulse pattern of a person is used to establish identity or provide authentication.

heuristics-based detection

See *behavior-based detection*.

hierarchical

A form of MAC environment. Hierarchical environments relate the various classification labels in an ordered structure from low security to medium security to high security. Each level or classification label in the structure is related. Clearance in a level grants the subject access to objects in that level as well as to all objects in all lower levels but prohibits access to all objects in higher levels.

hierarchical data model

A form of database that combines records and fields that are related in a logical tree structure. This is done so that each field can have one child or many or no children but each field can have only a single parent. Therefore, the data mapping relationship is one-to-many.

High-Speed Serial Interface (HSSI)

A layer 1 protocol used to connect routers and multiplexers to ATM or Frame Relay connection devices.

High-Level Data Link Control (HDLC)

A layer 2 protocol used to transmit data over synchronous communication lines. HDLC is an ISO standard based on IBM's SDLC. HDLC supports full-duplex communications, supports both point-to-point and multipoint connections, offers flow control, and includes error detection and correction.

high-level languages

Programming languages that are not machine languages or assembly languages. These languages are not hardware dependent and are more understandable by humans. Such languages must be converted to machine language before or during execution.

hijack attack

An attack in which a malicious user is positioned between a client and server and then interrupts the session and takes it over. Often, the malicious user impersonates the client so they can extract data from the server. The server is unaware that any change in the communication partner has occurred.

honey pot

Individual computers or entire networks created to serve as a snare for intruders. The honey pot looks and acts like a legitimate network, but it is 100 percent fake. Honey pots tempt intruders with unpatched and unprotected security vulnerabilities as well as hosting attractive, tantalizing, but faux data. Honey pots are designed to grab an intruder's attention and direct them into the restricted playground while keeping them away from the legitimate network and confidential resources.

host-based IDS

An intrusion detection system (IDS) that is installed on a single computer and can monitor the activities on that computer. A host-based IDS is able to pinpoint the files and processes compromised or employed by a malicious user to perform unauthorized activity.

hostile applet

Any piece of mobile code that attempts to perform unwanted or malicious activities.

hot site

A configuration in which a backup facility is maintained in constant working order, with a full complement of servers, workstations, and communications links ready to assume primary operations responsibilities.

hub

A network device used to connect multiple systems together in a star topology. Hubs repeat inbound traffic over all outbound ports.

hybrid

A type of MAC environment. A hybrid environment combines the hierarchical and compartmentalized concepts so that each hierarchical level can contain numerous subcompartments that are isolated from the rest of the security domain. A subject must have not only the correct clearance but also the need-to-know for the specific compartment in order to have access to the compartmentalized object.

hybrid attack

A form of password attack in which a dictionary attack is first attempted and then a type of brute-force attack is performed. The follow-up brute-force attack is used to add prefix or suffix characters to passwords from the dictionary in order to discover one-upped constructed passwords, two-upped constructed passwords, and so on.

Hypertext Transfer Protocol

The protocol used to transmit web page elements from a web server to web browsers (over the well-known service TCP/UDP port address 80).

Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)

A standard that uses port 443 to negotiate encrypted communications sessions between web servers and browser clients.

I

identification

The process by which a subject professes an identity and accountability is initiated. The identification process can consist of a user providing a username, a logon ID, a PIN, or a smart card or a process providing a process ID number.

identification card

A form of physical identification; generally contains a picture of the subject and/or a magnetic strip with additional information about a subject.

Identity Theft and Assumption Deterrence Act

An act that makes identity theft a crime against the person whose identity was stolen and provides severe criminal penalties (up to a 15-year prison term and/or a $250,000 fine) for anyone found guilty of violating it.

ignore risk

Denying that a risk exists and hoping that by ignoring a risk it will never be realized.

immediate addressing

A way of referring to data that is supplied to the CPU as part of an instruction.

impersonation

The assumption of someone's identity or online account, usually through the mechanisms of spoofing and session replay. An impersonation attack is considered a more active attack than masquerading.

implementation attack

This type of attack exploits weaknesses in the implementation of a cryptography system. It focuses on exploiting the software code, not just errors and flaws but methodology employed to program the encryption system.

inappropriate activities

Actions that may take place on a computer or over the IT infrastructure and that may not be actual crimes but are often grounds for internal punishments or termination. Some types of inappropriate activities include viewing inappropriate content, sexual and racial harassment, waste, and abuse.

incident

The occurrence of a system intrusion.

incremental backups

A backup that stores only those files that have been modified since the time of the most recent full or incremental backup. This is also used to mean the process of creating such a backup.

indirect addressing

The memory address that is supplied to the CPU as part of the instruction and doesn't contain the actual value that the CPU is to use as an operand. Instead, the memory address contains another memory address (perhaps located on a different page). The CPU then retrieves the actual operand from that address.

industrial espionage

The act of someone using illegal means to acquire competitive information.

inference

An attack that involves using a combination of several pieces of nonsensitive information to gain access to information that should be classified at a higher level.

inference engine

The second major component of an expert system that analyzes information in the knowledge base to arrive at the appropriate decision.

information flow model

A model that focuses on the flow of information to ensure that security is maintained and enforced no matter how information flows. Information flow models are based on a state machine model.

information hiding

Placing data and a subject at different security domains for the purpose of hiding the data from that subject.

informative policy

A policy that is designed to provide information or knowledge about a specific subject, such as company goals, mission statements, or how the organization interacts with partners and customers. An informative policy is nonenforceable.

inherit (or inheritance)

In object-oriented programming, inheritance refers to a class having one or more of the same methods from another class. So when a method has one or more of the same methods from another class, it is said to have “inherited” them.

initialization vector (IV)

A nonce used by numerous cryptography solutions to increase the strength of encrypted data by increasing the randomness of the input.

inrush

An initial surge of power usually associated with connecting to a power source, whether primary or alternate/secondary.

instance

In object-oriented programming, an instance can be an object, example, or representation of a class.

Integrated Services Digital Network (ISDN)

A digital end-to-end communications mechanism. ISDN was developed by telephone companies to support high-speed digital communications over the same equipment and infrastructure that is used to carry voice communications.

integrity

A state characterized by the assurance that modifications are not made by unauthorized users and authorized users do not make unauthorized modifications.

intellectual property

Intangible assets, such as secret recipes or production techniques.

International Data Encryption Algorithm (IDEA)

A block cipher that was developed in response to complaints about the insufficient key length of the DES algorithm. IDEA operates on 64-bit blocks of plain/cipher text, but it begins its operation with a 128-bit key.

International Organization for Standardization (ISO)

An independent oversight organization that defines and maintains computer, networking, and technology standards, along with more than 13,000 other international standards for business, government, and society.

Internet Key Exchange (IKE)

A protocol that provides for the secure exchange of cryptographic keys between IPSec participants.

Internet Message Access Protocol (IMAP)

A protocol used to transfer email messages from an email server to an email client.

Internet Security Association and Key Management Protocol (ISAKMP)

A protocol that provides background security support services for IPSec.

interpreted languages

Programming languages that are converted to machine language one command at a time at the time of execution.

interrupt (IRQ)

A mechanism used by devices and components in a computer to get the attention of the CPU.

intranet

A private network that is designed to host the same information services found on the Internet.

intrusion

The condition in which a threat agent has gained access to an organization’s infrastructure through the circumvention of security controls and is able to directly imperil assets. Also referred to as penetration.

intrusion detection

A specific form of monitoring both recorded information and real-time events to detect unwanted system access.

intrusion detection system (IDS)

A product that automates the inspection of audit logs and real-time system events. IDSs are generally used to detect intrusion attempts, but they can also be employed to detect system failures or rate overall performance.

IP header protocol field value

An element in an IP packet header that identifies the protocol used in the IP packet payload (usually this will be 6 for TCP, 17 for UDP, or 1 for ICMP, or any of a number of other valid routing protocol numbers).

IP Payload Compression (IPcomp) protocol

A protocol that allows IPSec users to achieve enhanced performance by compression packets prior to the encryption operation.

IP probes

An attack technique that uses automated tools to ping each address in a range. Systems that respond to the ping request are logged for further analysis. Addresses that do not produce a response are assumed to be unused and are ignored.

IP Security (IPSec)

A standards-based mechanism for providing encryption for point-to-point TCP/IP traffic.

IP spoofing

The process by which a malicious individual reconfigures their system so that it has the IP address of a trusted system and then attempts to gain access to other external resources.

iris scans

An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The colored portion of the eye that surrounds the pupil is used to establish identity or provide authentication.

isolation

A concept that ensures that any behavior will affect only the memory and resources associated with the process.

J

Java

A platform-independent programming language developed by Sun Microsystems.

job description

A detailed document outlining a specific position needed by an organization. A job description includes information about security classification, work tasks, and so on.

job responsibilities

The specific work tasks an employee is required to perform on a regular basis.

job rotation

A means by which an organization improves its overall security by rotating employees among numerous job positions. Job rotation serves two functions. First, it provides a type of knowledge redundancy. Second, moving personnel around reduces the risk of fraud, data modification, theft, sabotage, and misuse of information.

K

Kerchoff's assumption

The idea that all algorithms should be public but all keys should remain private. Kerchoff's assumption is held by a large number of cryptologists, but not all of them.

Kerberos

A ticket-based authentication mechanism that employs a trusted third party to provide identification and authentication.

kernel

The part of an operating system that always remains resident in memory (so that it can run on demand at any time).

kernel proxy firewalls

A firewall that is integrated into an operating system's core to provide multiple levels of session and packet evaluation. Kernel proxy firewalls are known as fifth-generation firewalls.

key

A secret value used to encrypt or decrypt messages.

key distribution center (KDC)

An element of the Kerberos authentication system. The KDC maintains all the secret keys of enrolled subjects and objects. A KDC is also a COMSEC facility that distributes symmetric crypto keys, especially for government entities.

key escrow system

A cryptographic recovery mechanism by which keys are stored in a database and can be recovered only by authorized key escrow agents in the event of key loss or damage.

keystroke dynamics

A biometric factor that measures how a subject uses a keyboard by analyzing flight time and dwell time.

keystroke monitoring

The act of recording the keystrokes a user performs on a physical keyboard. The act of recording can be visual (such as with a video recorder) or logical/technical (such as with a capturing hardware device or a software program).

keystroke patterns

An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The pattern and speed of a person typing a passphrase is used to establish identity or provide authentication.

knowledge base

A component of an expert system, the knowledge base contains the rules known by an expert system and seeks to codify the knowledge of human experts in a series of “if/then” statements.

knowledge-based detection

An intrusion discovery mechanism used by IDS and based on a database of known attack signatures. The primary drawback to a knowledge-based IDS is that it is effective only against known attack methods.

known plain-text attack

An attack in which the attacker has a copy of the encrypted message along with the plain-text message used to generate the cipher text (the copy). This greatly assists the attacker in breaking weaker codes.

KryptoKnight

A ticket-based authentication mechanism similar to Kerberos but based on peer-to-peer authentication.

L

LAN extender

A remote access, multilayer switch used to connect distant networks over WAN links. This is a strange beast of a device in that it creates WANs but marketers of this device steer clear of the term WAN and use only the terms LAN and extended LAN. The idea behind this device was to make the terminology easier to understand and thus make the device easier to sell than a more conventional WAN device grounded in complex concepts and terms.

land attack

A type of DoS. A land attack occurs when the attacker sends numerous SYN packets to a victim and the SYN packets have been spoofed to use the same source and destination IP address and port number as the victim's. This causes the victim to think it sent a TCP/IP session opening packet to itself, which causes a system failure, usually resulting in a freeze, crash, or reboot.

lattice-based access control

A variation of nondiscretionary access controls. Lattice-based access controls define upper and lower bounds of access for every relationship between a subject and object. These boundaries can be arbitrary, but they usually follow the military or corporate security label levels.

layer 1

The Physical layer of the OSI model.

layer 2

The Data Link layer of the OSI model.

layer 3

The Network layer of the OSI model.

layer 4

The Transport layer of the OSI model.

layer 5

The Session layer of the OSI model.

layer 6

The Presentation layer of the OSI model.

layer 7

The Application layer of the OSI model.

Layer 2 Forwarding (L2F)

A protocol developed by Cisco as a mutual authentication tunneling mechanism. L2F does not offer encryption.

Layer 2 Tunneling Protocol (L2TP)

A point-to-point tunnel protocol developed by combining elements from PPTP and L2F. L2TP lacks a built-in encryption scheme but typically relies upon IPSec as its security mechanism.

layering

The use of multiple security controls in series to provide for maximum effectiveness of security deployment.

learning rule

See *delta rule*.

licensing

A contract that states how a product is to be used.

lighting

One of the most commonly used forms of perimeter security control. The primary purpose of lighting is to discourage casual intruders, trespassers, prowlers, and would-be thieves who would rather perform their malicious activities in the dark.

link encryption

An encryption technique that protects entire communications circuits by creating a secure tunnel between two points. This is done by using either a hardware or software solution that encrypts all traffic entering one end of the tunnel and decrypts all traffic exiting the other end of the tunnel.

local alarm systems

Alarm systems that broadcast an audible signal that can be easily heard up to 400 feet away. Additionally, local alarm systems must be protected from tampering and disablement, usually by security guards. In order for a local alarm system to be effective, there must be a security team or guards positioned nearby who can respond when the alarm is triggered.

local area network (LAN)

A network that is geographically limited, such as within a single office, building, or city block.

log analysis

A detailed and systematic form of monitoring. The logged information is analyzed in detail to look for trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities.

logging

The activity of recording information about events or occurrences to a log file or database.

logic bomb

Malicious code objects that infect a system and lie dormant until they are triggered by the occurrence of one or more conditions.

logical access control

A hardware or software mechanism used to manage access to resources and systems and provide protection for them. They are the same as technical access controls. Examples of logical or technical access controls include encryption, smart cards, passwords, biometrics, constrained interfaces, access control lists, protocols, firewalls, routers, intrusion detection systems, and clipping levels.

logon credentials

The identity and the authentication factors offered by a subject to establish access.

logon script

A script that runs at the moment of user logon. A logon script is often used to map local drive letters to network shares, to launch programs, or to open links to often accessed systems.

loopback address

The IP address used to create a software interface that connects to itself via the TCP/IP protocol. The loopback address is handled by software alone. It permits testing of the TCP/IP protocol stack even if network interfaces or their device drivers are missing or damaged.

Low Water-Mark Mandatory Access Control (LOMAC)

A loadable kernel module for Linux designed to protect the integrity of processes and data. It is an OS security architecture extension or enhancement that provides flexible support for security policies.

M

machine language

A programming language that can be directly executed by a computer.

macro viruses

A virus that utilizes crude technologies to infect documents created in the Microsoft Word environment.

mail-bombing

An attack in which sufficient numbers of messages are directed to a single user's inbox or through a specific STMP server to cause a denial of service.

maintenance

The variety of tasks that are necessary to ensure continued operation in the face of changing operational, data processing, storage, and environmental requirements.

maintenance hooks

Entry points into a system that only the developer of the system knows; also called back doors.

malicious code

Code objects that include a broad range of programmed computer security threats that exploit various network, operating system, software, and physical security vulnerabilities to spread malicious payloads to computer systems.

mandatory access control

An access control mechanism that uses security labels to regulate subject access to objects.

mandatory vacations

A security policy that requires all employees to take vacations annually so their work tasks and privileges can be audited and verified. This often results in easy detection of abuse, fraud, or negligence.

man-in-the-middle attack

A type of attack that occurs when malicious users are able to position themselves between the two endpoints of a communication's link. The client and server are unaware that there is a third party intercepting and facilitating their communication session.

man-made disasters

Disasters cause by humans, including explosions, electrical fires, terrorist acts, power outages, utility failures, hardware/software failures, labor difficulties, theft, and vandalism.

mantrap

A double set of doors that is often protected by a guard. The purpose of a mantrap is to contain a subject until their identity and authentication is verified.

masquerading

Using someone else's security ID to gain entry into a facility or system.

massively parallel processing (MPP)

Technology used to create systems that house hundreds or even thousands of processors, each of which has its own operating system and memory/bus resources.

master boot record (MBR)

The portion of a hard drive or floppy disk that the computer uses to load the operating system during the boot process.

master boot record (MBR) virus

Virus that attacks the MBR. When the system reads the infected MBR, the virus instructs it to read and execute the code stored in an alternate location, thereby loading the entire virus into memory and potentially triggering the delivery of the virus's payload.

maximum tolerable downtime (MTD)

The maximum length of time a business function can be inoperable without causing irreparable harm to the business.

MD2 (Message Digest 2)

A hash algorithm developed by Ronald Rivest in 1989 to provide a secure hash function for 8-bit processors.

MD4

An enhanced version of the MD2 algorithm, released in 1990. MD4 pads the message to ensure that the message length is 64 bits smaller than a multiple of 512 bits.

MD5

The next version the MD algorithm, released in 1991, which processes 512-bit blocks of the message, but it uses four distinct rounds of computation to produce a digest of the same length as the MD2 and MD4 algorithms (128 bits).

mean time to failure (MTTF)

The length of time or number of uses a hardware or media component can endure before its reliability is questionable and it should be replaced.

Media Access Control (MAC) address

A 6-byte address written in hexadecimal. The first three bytes of the address indicate the vendor or manufacturer of the physical network interface. The last three bytes make up a unique number assigned to that interface by the manufacturer. No two devices on the same network can have the same MAC address.

meet-in-the-middle attack

An attack in which the attacker uses a known plain-text message. The plain text is then encrypted using every possible key (k1), while the equivalent cipher text is decrypted using all possible keys (k2).

memory

The main memory resources directly available to a system’s CPU. Primary memory normally consists of volatile random access memory (RAM) and is usually the most high-performance storage resource available to a system.

memory card

A device that can store data but cannot process it; often built around some form of flash memory.

memory page

A single chunk of memory that can be moved to and from RAM and the paging file on a hard drive as part of a virtual memory system.

memory-mapped I/O

A technique used to manage input/output between system components and the CPU.

message

The communications to or input for an object (in the context of object-oriented programming terminology and concepts).

message digest (MD)

A summary of a message's content (not unlike a file checksum) produced by a hashing algorithm.

metadata

The results of a data mining operation on a data warehouse.

metamodel

A model of models. Because the spiral model encapsulates a number of iterations of another model (the waterfall model), it is known as a metamodel.

methods

The actions or functions performed on input (messages) to produce output (behaviors) by objects in an object-oriented programming environment.

microcode

A term used to describe software that is stored in a ROM chip. Also called firmware.

middle management

See *security professional*.

military and intelligence attacks

Attacks that are launched primarily to obtain secret and restricted information from law enforcement or military and technological research sources.

MIME Object Security Services (MOSS)

Standard that provides authenticity, confidentiality, integrity, and nonrepudiation for email messages.

mitigated

The process by which a risk is reduced or removed.

mitigate risk

See *reducing risk*.

mobile sites

Nonmainstream alternatives to traditional recovery sites that typically consist of self-contained trailers or other easily relocated units.

module testing

When each independent or self-contained segment of code for which there exists a distinct and separate specification is tested independently of all other modules. This can also be called component testing. This can be seen as a parent or superclass of unit testing.

modulo

The remainder value left over after a division operation is performed.

MONDEX

A type of electronic payment system and protocol designed to manage cash on smart cards.

monitoring

The activity of manually or programmatically reviewing logged information looking for specific information.

motion detector

A device that senses the occurrence of motion in a specific area.

motion sensor

See *motion detector*.

multicast

A communications transmission to multiple identified recipients.

multilevel mode

See *multilevel security mode*.

multilevel security mode

A system that is authorized to process information at more than one level of security even when all system users do not have appropriate clearances or a need to know for all information processed by the system.

multipartite virus

A virus that uses more than one propagation technique in an attempt to penetrate systems that defend against only one method or the other.

multiprocessing

A technology that makes it possible for a computing system to harness the power of more than one processor to complete the execution of a single application.

multiprogramming

The pseudo-simultaneous execution of two tasks on a single processor coordinated by the operating system for the purpose of increasing operational efficiency. Multiprogramming is considered a relatively obsolete technology and is rarely found in use today except in legacy systems.

multistate

Term used to describe a system that is certified to handle multiple security levels simultaneously by using specialized security mechanisms that are designed to prevent information from crossing between security levels.

multitasking

A system handling two or more tasks simultaneously.

multithreading

A process that allows multiple users to use the same process without interfering with each other.

mutual assistance agreement (MAA)

An agreement in which two organizations pledge to assist each other in the event of a disaster by sharing computing facilities or other technological resources.

N

natural disaster

A disaster that is not caused by man, such as earthquakes, mud slides, sink holes, fires, floods, hurricanes, tornadoes, falling rocks, snow, rainfall, ice, humidity, heat, extreme cold, and so on.

need-to-know

The requirement to have access to, knowledge about, or possession of data or a resource in order to perform specific work tasks. A user must have a need to know in order to gain access to data or resources. Even if that user has an equal or greater security classification than the requested information, if they do not have a need to know, they are denied access.

negligence

Failure to exercise the degree of care considered reasonable under the circumstances, resulting in an unintended injury to another party.

Network Address Translation (NAT)

A mechanism for converting the internal private IP addresses found in packet headers into public IP addresses for transmission over the Internet.

Network layer

Layer 3 of the OSI model.

network-based IDS

An IDS installed onto a host to monitor a network. Network-based IDSs detect attacks or event anomalies through the capture and evaluation of network packets.

neural network

A system in which a long chain of computational decisions that feed into each other and eventually add up to produce the desired output is set up.

noise

A steady interfering disturbance.

nonce

A random number generator variable used in cryptography software and creates a new and unique value every time it is used often based on a timestamp based seed value.

nondisclosure agreement (NDA)

A document used to protect the confidential information within an organization from being disclosed by a former employee. When a person signs an NDA, they agree not to disclose any information that is defined as confidential to anyone outside of the organization. Often, violations of an NDA are met with strict penalties.

nondiscretionary access control

An access control mechanism that regulates subject access to objects by using roles or tasks.

noninterference model

A model loosely based on the information flow model. The noninterference model is concerned with the actions of one subject affecting the system state or actions of another subject.

nonrepudiation

A feature of a security control or an application that prevents the sender of a message or the subject of an activity or event from denying that the event occurred.

nonvolatile

See *nonvolatile storage*.

nonvolatile storage

A storage system that does not depend upon the presence of power to maintain its contents, such as magnetic/optical media and nonvolatile RAM (NVRAM).

normalization

The database process that removes redundant data and ensures that all attributes are dependent on the primary key.

NOT

An operation (represented by the ~ or ! symbol) that reverses the value of an input variable. This function operates on only one variable at a time.

O

object

A passive entity that provides information or data to subjects. An object can be a file, a database, a computer, a program, a process, a file, a printer, a storage media, and so on.

object linking and embedding (OLE)

A Microsoft technology used to link data objects into or from multiple files or sources on a computer.

object-oriented programming (OOP)

A method of programming that uses encapsulated code sets called objects. OOP is best suited for eliminating error propagation and mimicking or modeling the real world.

object-relational database

A relational database combined with an object-oriented programming environment.

one-time pad

An extremely powerful type of substitution cipher that uses a different key for each message. The key length is the same length as the message.

one-time password

A variant of dynamic passwords that is changed every time it is used.

one-upped constructed password

A password with a single-character difference from its present form in a dictionary list.

one-way encryption

A mathematical function performed on passwords, messages, CRCs, and so on, that creates a cryptographic code that cannot be reversed.

one-way function

A mathematical operation that easily produces output values for each possible combination of inputs but makes it impossible to retrieve the input values. Public key cryptosystems are all based upon some sort of one-way function.

open system authentication (OSA)

A connection scheme for wireless networks where no real authentication is required, as long as a radio signal can be transmitted between the client and WAP, then communications are allowed.

Open Systems Interconnection (OSI) model

A standard model developed to establish a common communication structure or standard for all computer systems.

operational plans

Short-term and highly detailed plans based on the strategic and tactical plans. Operational plans are valid or useful only for a short time. They must be updated often (such as monthly or quarterly) to retain compliance with tactical plans. Operational plans are detailed plans on how to accomplish the various goals of the organization.

operations security triple

The relationship between asset, vulnerability, and threat.

OR

An operation (represented by the ∨ symbol) that checks to see whether at least one of the input values is true.

organizational owner

See *senior management*.

Orthogonal Frequency-Division Multiplexing (OFDM)

A wireless technology that employs a digital multicarrier modulation scheme that allows for a more tightly compacted transmission.

OSI model

See *Open Systems Interconnection (OSI) model*.

Output Feedback (OFB)

A mode in which DES XORs plain text with a seed value. For the first encrypted block, an initialization vector is used to create the seed value. Future seed values are derived by running the DES algorithm on the preceding seed value. The major advantage of OFB mode is that transmission errors do not propagate to affect the decryption of future blocks.

overt channel

An obvious, visible, detectable, known method of communicating that is addressed by a security policy and subsequently controlled by logical or technical access controls.

overwriting

See *clearing*.

owner

The person who has final corporate responsibility for the protection and storage of data. The owner may be liable for negligence if they fail to perform due diligence in establishing and enforcing security policy to protect and sustain sensitive data. The owner is typically the CEO, president, or department head.

P

package

In the context of the Common Criteria for information technology security evaluation, a package is a set of security features that can be added or removed from a target system.

packet

A portion of a message that contains data and the destination address; also called a datagram.

padded cell

Similar to a honey pot. When an intruder is detected by an IDS, the intruder is transferred to a padded cell. The padded cell has the look and layout of the actual network, but within the padded cell the intruder can neither perform malicious activities nor access any confidential data. A padded cell is a simulated environment that may offer fake data to retain an intruder's interest.

palm geography

An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The shape of a person's hand is used to establish identity or provide authentication.

palm scan

See *palm topography*.

palm topography

An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The layout of ridges, creases, and grooves on a person's palm is used to establish identity or provide authentication. This is the same as a palm scan and similar to a fingerprint.

parallel run

A type of new system deployment testing in which the new system and the old system are run in parallel.

parallel tests

Testing that involves actually relocating personnel to an alternate recovery site and implementing site activation procedures.

parole evidence rule

An rule that states that when an agreement between parties is put into written form, the written document is assumed to contain all the terms of the agreement and no verbal agreements may modify the written agreement.

partial-knowledge teams

Possess a detailed account of organizational assets, including hardware and software inventory, prior to a penetration test.

passphrase

A string of characters usually much longer than a password. Once the passphrase is entered, the system converts it into a virtual password for use by the authentication process. Passphrases are often natural-language sentences to allow for simplified memorization.

password

A string of characters entered by a subject as an authentication factor.

Password Authentication Protocol (PAP)

A standardized authentication protocol for PPP. PAP transmits usernames and passwords in the clear. PAP offers no form of encryption; it simply provides a means to transport the logon credentials from the client to the authentication server.

password policy

The section of an organization’s security policy that dictates the rules, restrictions, and requirements of passwords. This can also indicate the programmatic controls deployed on a system to improve the strength of passwords.

password restrictions

The rules that define the minimal requirements of passwords, such as length, character composition, and age.

patent

A governmental grant that bestows upon an invention’s creator the sole right to make, use, and sell that invention for a set period of time.

pattern-matching detection

See *knowledge-based detection*.

penetration

See *intrusion*.

penetration testing

An activity used to test the strength and effectiveness of deployed security measures with an authorized attempted intrusion attack. Penetration testing should be performed only with the consent and knowledge of the management staff.

permanent virtual circuit (PVC)

A predefined virtual circuit that is always available for a Frame Relay customer.

personal identification number (PIN)

A number or code assigned to a person to be used as an identification factor. PINs should be kept secret.

personnel management

An important factor in maintaining operations security. Personnel management is a form of administrative control or administrative management.

phone phreaking

The process of breaking into telephone company computers to place free calls.

physical access control

A physical barrier deployed to prevent direct contact with systems. Examples of physical access controls include guards, fences, motion detectors, locked doors, sealed windows, lights, cable protection, laptop locks, swipe cards, dogs, CCTV, mantraps, and alarms.

physical controls for physical security

See *physical access control*.

Physical layer

Layer 1 of the OSI model.

piggybacking

The act of following someone through a secured gate or doorway without being identified or authorized personally.

ping

A utility used to troubleshoot a connection to test whether a particular IP address is accessible.

ping-of-death attack

A type of DoS. A ping-of-death attack employs an oversized ping packet. Using special tools, an attacker can send numerous oversized ping packets to a victim. In many cases, when the victimized system attempts to process the packets, an error occurs causing the system to freeze, crash, or reboot.

plain old telephone service (POTS)

Normal telephone service.

plaintext

A message that has not been encrypted.

playback attack

See *replay attack*.

Point-to-Point Protocol (PPP)

A full-duplex protocol used for the transmission of TCP/IP packets over various non-LAN connections, such as modems, ISDN, VPNs, Frame Relay, and so on. PPP is widely supported and is the transport protocol of choice for dial-up Internet connections.

Point-to-Point Tunneling Protocol (PPTP)

An enhancement of PPP that creates encrypted tunnels between communication endpoints. PPTP is used on VPNs but is often replaced by L2TP.

policy

See *security policy*.

polyalphabetic substitution

A cryptographic transformation that encrypts a message using letter-by-letter conversion and multiple alphabets from different languages or countries.

polyinstantiation

The event that occurs when two or more rows in the same table appear to have identical primary key elements but contain different data for use at differing classification levels. Polyinstantiation is often used as a defense against some types of inference attacks.

polymorphic virus

A virus that modifies its own code as it travels from system to system. The virus’s propagation and destruction techniques remain the same, but the signature of the virus is somewhat different each time it infects a new system.

polymorphism

In the context of object-oriented programming terminology and concepts, the characteristic of an object to provide different behaviors based upon the same message and methods owing to variances in external conditions.

port

A connection address within a protocol.

Port Address Translation (PAT)

A mechanism for converting the internal private IP addresses found in packet headers into public IP addresses and port numbers for transmission over the Internet. PAT supports a many-to-one mapping of internal to external IP addresses by using ports.

port scan

Software used by an intruder to probe all of the active systems on a network and determine what public services are running on each machine.

postmortem review

An analysis and review of an activity after its completion to determine its success and whether processes and procedures need to be improved.

Post Office Protocol (POP)

A protocol used to transfer email messages from an email server to an email client.

preaction system

A combination dry pipe/wet pipe system. The system exists as a dry pipe until the initial stages of a fire (smoke, heat, and so on) are detected and then the pipes are filled with water. The water is released only after the sprinkler head activation triggers are melted by sufficient heat. If the fire is quenched before the sprinklers are triggered, the pipes can be manually emptied and reset. This also allows for manual intervention to stop the release of water before sprinkler triggering occurs. Preaction systems are the most appropriate water-based system for environments that include both computers and humans in the same locations.

Presentation layer

Layer 6 of the OSI model.

Pretty Good Privacy (PGP)

A public/private key system that uses the IDEA algorithm to encrypt files and email messages. PGP is not a standard but rather an independently developed product that has wide Internet grassroots support.

preventative access control

See *preventive access control*.

preventive access control

An access control deployed to stop an unwanted or unauthorized activity from occurring. Examples of preventive access controls include fences, security policies, security awareness training, and antivirus software.

preventive control

Any security mechanism, tool, or practice that can deter and mitigate undesirable actions or events.

primary memory

Storage that normally consists of volatile random access memory (RAM) and is usually the most high-performance storage resource available to a system.

Primary Rate Interface (PRI)

An ISDN service type that provides up to 23 B channels and one D channel. Thus, a full PRI ISDN connection offers 1.544 Mbps throughput, the same as a T1 line.

primary storage

The RAM that a computer uses to keep necessary information readily available.

principle of least privilege

An access control philosophy that states that subjects are granted the minimal access possible for the completion of their work tasks.

privacy

An element of confidentiality aimed at preventing personal or sensitive information about an individual or organization from being disclosed.

Privacy Act of 1974

A law that mandates that government agencies maintain only records that are necessary for the conduct of their business and destroy those records when they are no longer needed for a legitimate function of government. It provides a formal procedure for individuals to gain access to records the government maintains about them and to request that incorrect records be amended. The Privacy Act also restricts the way the federal government can deal with private information about individual citizens.

Privacy Enhanced Mail (PEM)

An email encryption mechanism that provides authentication, integrity, confidentiality, and nonrepudiation. PEM is a layer 7 protocol. PEM uses RSA, DES, and X.509.

private

A commercial business/private sector classification used for data of a private or personal nature that is intended for internal use only. A significant negative impact could occur for the company or individuals if private data is disclosed.

private branch exchange (PBX)

A sophisticated telephone system often used by organizations to provide inbound call support, extension-to-extension calling, conference calling, and voicemail. This can be implemented as a stand-alone phone system network or can be integrated with the IT infrastructure.

private IP addresses

The addresses defined in RFC 1918, which are not routed over the Internet.

private key

A secret value that is used to encrypt or decrypt messages and is kept secret and known only to the user; used in conjunction with a public key in asymmetrical cryptography.

privileged entity controls

See *privileged operations functions*.

privileged mode

The mode designed to give the operating system access to the full range of instructions supported by the CPU.

privileged operations functions

Activities that require special access or privilege to perform within a secured IT environment. In most cases, these functions are restricted to administrators and system operators.

problem state

The state in which a process is actively executing.

procedure

In the context of security, a detailed step-by-step how-to document describing the exact actions necessary to implement a specific security mechanism, control, or solution.

process isolation

One of the fundamental security procedures put into place during system design. Basically, using process isolation mechanisms (whether part of the operating system or part of the hardware itself) ensures that each process has its own isolated memory space for storage of data and the actual executing application code itself.

processor

The central processing unit in a PC; it handles all functions on the system.

Program Evaluation Review Technique (PERT)

A project-scheduling tool. It is a method used to judge the size of a software product in development and calculate the standard deviation (SD) for risk assessment. PERT relates the estimated lowest possible size, the most likely size, and the highest possible size of each component. PERT is used to direct improvements to project management and software coding in order to produce more efficient software. As the capabilities of programming and management improve, the actual produced size of software should be smaller.

programmable read-only memory (PROM)

A PROM chip that does not have its contents “burned in” at the factory as is done with standard ROM chips. Instead, special functionality is installed that allows the end user to burn in the contents of the chip.

proprietary

A form of commercial business/private sector confidential information. If proprietary data is disclosed, it can have drastic effects on the competitive edge of an organization.

protection profile

From the Common Criteria for information technology security evaluation, the evaluation element in which a subject states its security needs.

protocol

A set of rules and restrictions that define how data is transmitted over a network medium (for example, twisted-pair cable, wireless transmission, and so on). Protocols make computer-to-computer communications possible.

proximity reader

A passive device, field-powered device, or transponder that detects the presence of authorized personnel and grants them physical entry into a facility. The proximity device is worn or held by the authorized bearer. When they pass a proximity reader, the reader is able to determine who the bearer is and whether they have authorized access.

proxy

A mechanism that copies packets from one network into another. The copy process also changes the source and destination address to protect the identity of the internal or private network.

prudent man rule

Invoked by the Federal Sentencing Guidelines, the rule that requires senior officials to perform their duties with the care that ordinary, prudent people would exercise under similar circumstances.

pseudo-flaws

A technique often used on honey pot systems and on critical resources to emulate well-known operating system vulnerabilities.

public

The lowest level of commercial business/private sector classification. Used for all data that does not fit in one of the higher classifications. This information is not readily disclosed, but if it is, it should not have a serious negative impact on the organization.

public key

A value that is used to encrypt or decrypt messages and is made public to any user and used with a private key in asymmetric cryptography.

public key infrastructure (PKI)

A hierarchy of trust relationships that makes it possible to facilitate communication between parties previously unknown to each other.

purging

The process of erasing of media so it can be reused in a less secure environment.

Q

qualitative decision making

A decision making process that takes nonnumerical factors, such as emotions, investor/customer confidence, workforce stability, and other concerns, into account. This type of data often results in categories of prioritization (such as high, medium, and low).

qualitative risk analysis

Scenario-oriented analysis using ranking and grading for exposure ratings and decisions.

quality assurance check

A form of personnel management and project management that oversees the development of a product. QA checks ensure that the product in development is consistent with stated standards, methods of practice, efficiency, and so on.

quantitative decision making

The use of numbers and formulas to reach a decision. Options are often expressed in terms of the dollar value to the business.

quantitative risk analysis

A method that assigns real dollar figures to the loss of an asset.

R

radiation monitoring

A specific form of sniffing or eavesdropping that involves the detection, capture, and recording of radio frequency signals and other radiated communication methods, including sound and light.

radio frequency identification (RFID)

A technology that uses electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to identify a specific device. Each RFID tag includes a unique identifier, so that when a nearby antenna/transceiver actives the tag, it transmits that identifier back to the antenna where that value is recorded, or used to trigger some kind of action. For example, most modern toll-road systems use RFID devices that drivers attach to the windshields of their cars, and each time a device is “read” by an antenna, the vehicle owner’s toll balance is incremented by the cost of that transit. RFID devices may also be used to track individuals (carrying tags), equipment (bearing tags), and so forth, within the premises of an enterprise for security monitoring.

radio frequency interference (RFI)

A type of noise that is generated by a wide number of common electrical appliances, including fluorescent lights, electrical cables, electric space heaters, computers, elevators, motors, electric magnets, and so on. RFI can affect many of the same systems EMI affects.

RADIUS

See *Remote Authentication Dial-In User Service (RADIUS)*.

random access memory (RAM)

Readable and writable memory that contains information the computer uses during processing. RAM retains its contents only when power is continuously supplied to it.

random access storage

Devices, such as RAM and hard drives, that allow the operating system to request contents from any point within the media.

read-only memory (ROM)

Memory that can be read but cannot be written to.

ready state

The state in which a process is ready to execute but is waiting for its turn on the CPU.

real evidence

Items that can actually be brought into a court of law; also known as object evidence.

real memory

Typically the largest RAM storage resource available to a computer. It is normally composed of a number of dynamic RAM chips and therefore must be refreshed by the CPU on a periodic basis; also known as main memory or primary memory.

realized risk

The incident, occurrence, or event when a risk becomes a reality and a breach, attack, penetration, or intrusion has occurred that may or may not result in loss, damage, or disclosure of assets.

record

Contents of a table in a relational database.

record retention

The organizational policy that defines what information is maintained and for how long. In most cases, the records in question are audit trails of user activity. This may include file and resource access, logon patterns, email, and the use of privileges.

record sequence checking

Similar to hash total checking, but instead of verifying content integrity, it involves verifying packet or message sequence integrity.

recovery access control

A type of access control that is used to repair or restore resources, functions, and capabilities after a security policy violation.

recovery strategies

The practices, policies, and procedures to recover a business that include designating first responders to major incidents, performing critical follow-up tasks, and obtaining insurance to reduce risk of financial loss.

recovery time objective (RTO)

See *maximum tolerable downtime (MTD)*.

reducing risk

The implementation of safeguards and countermeasures. Also referred to as mitigating risk.

reference monitor

A portion of the security kernel that validates user requests against the system's access control mechanisms.

reference profile

The digitally stored sample of a biometric factor.

reference template

See *reference profile*.

referential integrity

Used to enforce relationships between two tables. One table in the relationship contains a foreign key that corresponds to the primary key of the other table in the relationship.

register

A limited amount of onboard memory in a CPU.

register address

The address of a register, which is a small memory location directly on the CPU. When the CPU needs information from one of those registers to complete an operation, it can simply use the register address (for example, "register one") to access the information.

registration authority (RA)

A read-only version of a certificate authority that is able to distribute the CRL and perform certificate verification processes but is not able to create new certificates. An RA is used to share the workload of a CA.

regulatory policy

A policy that is required whenever industry or legal standards are applicable to your organization. This policy discusses the regulations that must be followed and outlines the procedures that should be used to elicit compliance.

reject risk

To deny that a risk exists or hope that by ignoring a risk, it will never be realized. It is an unacceptable response to risk. Also referred to as deny risk.

relational database

A database that consists of tables that contain a set of related records.

relationship

The association of information in tables of a relational database.

relevant

Characteristic of evidence that is applicable in determining a fact in a court of law.

Remote Authentication Dial-In User Service (RADIUS)

A service used to centralize the authentication of remote dial-up connections.

remote journaling

Transferring copies of the database transaction logs containing the transactions that occurred since the previous bulk transfer.

remote mirroring

Maintaining a live database server at the backup site. It is the most advanced database backup solution.

repeater

A network device used to amplify signals on network cabling to allow for longer distances between nodes. Can also be called a concentrator or amplifier.

replay attack

An attack in which a malicious user records the traffic between a client and server. The packets sent from the client to the server are then played back or retransmitted to the server with slight variations of the time stamp and source IP address (in other words, spoofing). In some cases, this allows the malicious user to restart an old communication link with a server. Also referred to as a playback attack.

residual risk

Risk that comprises specific threats to specific assets against which upper management chooses not to implement a safeguard. In other words, residual risk is the risk that management has chosen to accept rather than mitigate.

restricted interface model

A model that uses classification-based restrictions to offer only subject-specific authorized information and functions. One subject at one classification level will see one set of data and have access to one set of functions while another subject at a different classification level will see a different set of data and have access to a different set of functions.

retina scan

An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The blood vessel pattern at the back of the eyeball is used to establish identity or provide authentication.

Reverse Address Resolution Protocol (RARP)

A subprotocol of the TCP/IP protocol suite that operates at the Data Link layer (layer 2). RARP is used to discover the IP address of a system by polling using its MAC address.

reverse engineering

This is considered an unethical form of engineering. Programmers decompile code to understand all the intricate details of its functionality, especially when employed for the purpose of creating a similar, competing, or compatible product.

reverse hash matching

The process of discovering the original message that has been hashed by generating potential messages, hashing them, and comparing their hash value to the original. When H(M) = H(M'), then M = M'.

revocation

A mechanism that allows a PKI certificate to be canceled, effectively removing a user from the system.

RFC 1918

The public standard that defines public and private IP addresses.

Rijndael block cipher

A block cipher that was selected to replace DES. The Rijndael cipher allows the use of three key strengths: 128 bits, 192 bits, and 256 bits.

risk

The likelihood that any specific threat will exploit a specific vulnerability to cause harm to an asset. Risk is an assessment of probability, possibility, or chance. Risk = threat * vulnerability.

risk analysis

An element of risk management that includes analyzing an environment for risks, evaluating each risk as to its likelihood of occurring and cost of damage, assessing the cost of various countermeasures for each risk, and creating a cost/benefit report for safeguards to present to upper management.

risk management

A detailed process of identifying factors that could damage or disclose data, evaluating those factors in light of data value and countermeasure cost, and implementing cost-effective solutions for mitigating or reducing risk.

risk tolerance

The ability of an organization to absorb the losses associated with realized risks.

Rivest, Shamir, and Adleman (RSA)

A public key encryption algorithm named after Rivest, Shamir, and Adleman, its inventors.

role-based access control

A form of nondiscretionary access controls that employs job function roles to regulate subject access to objects.

root

The administrator level of a system.

rootkit

A specialized software package that allows hackers to gain expanded access to a system.

router

A network device used to control traffic flow on networks. Routers are often used to connect similar networks together and control traffic flow between them. They can function using statically defined routing tables or employ a dynamic routing system.

RSA

See *Rivest, Shamir, and Adleman (RSA)*.

rule-based access control

A variation of mandatory access controls. A rule-based system uses a set of rules, restrictions, or filters to determine what can and cannot occur on the system, such as granting subject access, performing an action on an object, or accessing a resource. Firewalls, proxies, and routers are common examples of rule-based access control systems.

running key cipher

A form of cryptography in which the key is a designation of a changing source, such as the third page of the *New York Times*.

running state

The state in which a process is actively executing. This is another name for problem state.

S

S/MIME

See *Secure Multipurpose Internet Mail Extensions (S/MIME)*.

sabotage

A criminal act committed against an organization by a knowledgeable employee.

safeguard

Anything that removes a vulnerability or protects against one or more specific threats. Also referred to as a countermeasure.

sag

Momentary low voltage.

salami attack

An attack performed by gathering small amounts of data to construct something of greater value or higher sensitivity.

salt

A random number appended to a password before hashing to increase randomness and ensure uniqueness in the resulting stored hash value.

sampling

A form of data reduction that allows an auditor to quickly determine the important issues or events from an audit trail.

sandbox

A security boundary within which a Java applet executes.

sanitization

Any number of processes that prepares media for destruction. Sanitization is the process that ensures that data cannot be recovered by any means from destroyed or discarded media. Sanitization can also be the actual means by which media is destroyed. Media can be sanitized by purging or degaussing without physically destroying the media.

scanning

Similar to “casing” a neighborhood prior to a burglary, the process by which a potential intruder looks for possible entryways into a system. Scanning can indicate that illegal activity will follow, so it is a good idea to treat scans as incidents and to collect evidence of scanning activity.

scavenging

A form of dumpster diving performed electronically. Online scavenging searches for useful information in the remnants of data left over after processes or tasks are completed. This could include audit trails, log files, memory dumps, variable settings, port mappings, cached data, and so on.

schema

The structure that holds the data that defines or describes a database. The schema is written using a Data Definition Language (DDL).

scripted access

A method to automate the logon process with a script that provides the logon credentials to a system. It is considered a form of single sign-on.

search warrant

A document obtained through the judicial system that allows law enforcement personnel to acquire evidence from a location without first alerting the individual believed to have perpetrated a crime.

secondary evidence

A copy of evidence or an oral description of the contents of best evidence.

secondary memory

Magnetic/optical media and other storage devices that contain data not immediately available to the CPU.

secondary storage

Data repositories that include magnetic and optical media, such as tapes, disks, hard drives, and CD/DVD storage.

second-tier attack

An assault that relies upon information or data gained from eavesdropping or other similar data-gathering techniques. In other words, it is an attack that is launched only after some other attack is completed.

Secret

A government/military classification, used for data of a secret nature. Unauthorized disclosure of secret data could cause serious damage to national security.

secure communication protocol

A protocol that uses encryption to provide security for the data transmitted by it.

Secure Electronic Transaction (SET)

A security protocol for the transmission of transactions over the Internet. SET is based on RSA encryption and DES. SET had the support of major credit card companies, such as Visa and MasterCard. However, it has mostly been abandoned in light of newer and more secure alternatives.

Secure Hash Algorithm (SHA)

A government standard hash function developed by the National Institute of Standards and Technology (NIST) and specified in an official government publication.

Secure HTTP (S-HTTP)

The second major protocol used to provide security on the World Wide Web.

Secure Multipurpose Internet Mail Extensions (S/MIME)

A protocol used to secure the transmission of email and attachments.

Secure Remote Procedure Call (S-RPC)

An authentication service. S-RPC is simply a means to prevent unauthorized execution of code on remote systems.

Secure Shell (SSH)

An end-to-end encryption technique. This suite of programs provides encrypted alternatives to common Internet applications such as FTP, Telnet, and rlogin. There are actually two versions of SSH. SSH1 supports the DES, 3DES, IDEA, and Blowfish algorithms. SSH2 drops support for DES and IDEA but adds support for several other algorithms.

Secure Sockets Layer (SSL)

An encryption protocol developed by Netscape to protect the communications between a web server and a web browser.

security association (SA)

In an IPSec session, the representation of the communication session and process of recording any configuration and status information about the connection.

security ID

A form of physical identification; generally contains a picture of the subject and/or a magnetic strip with additional information about a subject.

security kernel

The core set of operating system services that handles all user/application requests for access to system resources.

security label

An assigned classification or sensitivity level used in security models to determine the level of security required to protect an object and prevent unauthorized access.

security management planning

The act of thoroughly and systematically designing procedural and policy documentation to reduce risk and then to maintain risk at an acceptable level for a given environment.

security perimeter

The imaginary boundary that separates the trusted computing base from the rest of the system.

security policy

A document that defines the scope of security needs of an organization, prescribes solutions to manage security issues, and discusses the assets that need protection and the extent to which security solutions should go to provide the necessary protection.

security professional

Trained and experienced network, systems, and security engineer who is responsible for following the directives mandated by senior management.

security role

The part an individual plays in the overall scheme of security implementation and administration within an organization.

security target

The evaluation element from the Common Criteria for information technology security evaluation in which a vendor states the security features of its product.

senior management

A person or group who is ultimately responsible for the security maintained by an organization and who should be most concerned about the protection of its assets. They must sign off on all policy issues, and they will be held liable for overall success or failure of a security solution. It is the responsibility of senior management to show prudent due care. Also referred to as organizational owner and upper management.

sensitive

A commercial business/private sector classification used for data that is more sensitive than public data. A negative impact could occur for the company if sensitive data is disclosed.

sensitive but unclassified

A government/military classification used for data of a sensitive or private nature but significant damage would not occur if disclosed.

sensitivity

In regard to biometric devices, the level at which the device is configured for scanning.

separation of duties and responsibilities

A common practice to prevent any single subject from being able to circumvent or disable security mechanisms. By dividing core administration or high-authority responsibilities among several subjects, no one subject has sufficient access to perform significant malicious activities or bypass imposed security controls.

separation of privilege

The principle that builds upon the principle of least privilege. It requires the use of granular access permissions; that is, different permissions for each type of privileged operation. This allows designers to assign some processes rights to perform certain supervisory functions without granting them unrestricted access to the system.

Sequenced Packet Exchange (SPX)

The Transport layer protocol of the IPX/SPX protocol suite from Novell.

sequential storage

Devices that require that you read (or speed past) all of the data physically stored prior to the desired location. A common example of a sequential storage device is a magnetic tape drive.

Serial Line Internet Protocol (SLIP)

An older technology developed to support TCP/IP communications over asynchronous serial connections, such as serial cables or modem dial-up.

service bureaus

Businesses that lease computer time through contractual agreements and provide all IT needs in the event of some disaster or business interruption that requires a disaster recovery plan or business continuity plan to be enacted.

service-level agreement (SLA)

A contractual obligation to your clients that requires you to implement sound BCP practices. Also used to assure acceptable levels of service from suppliers for sound BCP practices.

SESAME

A ticket-based authentication mechanism similar to Kerberos.

session hijacking

An attack that occurs when a malicious individual intercepts part of a communication between an authorized user and a resource and then uses a hijacking technique to take over the session and assume the identity of the authorized user.

Session layer

Layer 5 of the OSI model.

shared key authentication (SKA)

A connection scheme for wireless networks that requires that some form of authentication must take place before network communications can occur. The 802.11 standard defines one optional technique for SKA known as WEP.

shielded twisted-pair (STP)

A twisted-pair wire that includes a metal foil wrapper inside the outer sheath to provide additional protection from EMI.

shoulder surfing

The act of gathering information from a system by observing the monitor or the use of the keyboard by the operator.

shrink-wrap license agreement

A license written on the outside of software packaging. Such licenses get their name because they commonly include a clause stating that you acknowledge agreement to the terms of the contract simply by breaking the shrink-wrap seal on the package.

signature-based detection

The process used by antivirus software to identify potential virus infections on a system.

signature dynamics

When used as a biometric, the use of the pattern and speed of a person writing their signature to establish identity or provide authentication.

Simple Integrity Axiom (SI Axiom)

An axiom of the Biba model that states that a subject at a specific classification level cannot read data with a lower classification level. This is often shortened to “no read down.”

Simple Key Management for IP (SKIP)

An encryption tool used to protect sessionless datagram protocols.

Simple Mail Transfer Protocol (SMTP)

The primary protocol used to move email messages from clients to servers and from server to server.

Simple Security Property (SS property)

A property of the Bell-LaPadula model that states that a subject at a specific classification level cannot read data with a higher classification level. This is often shortened to “no read up.”

simulation tests

A test in which disaster recovery team members are presented with a scenario and asked to develop an appropriate response. Some of these response measures are then tested. This may involve the interruption of noncritical business activities and the use of some operational personnel.

single loss expectancy (SLE)

The cost associated with a single realized risk against a specific asset. The SLE indicates the exact amount of loss an organization would experience if an asset were harmed by a specific threat. SLE = asset value ($) * exposure factor (EF).

single sign-on (SSO)

A mechanism that allows subjects to authenticate themselves only once to a system. With SSO, once subjects are authenticated, they can freely roam the network and access resources and service without being rechallenged for authentication.

single state

Systems that require the use of policy mechanisms to manage information at different levels. In this type of arrangement, security administrators approve a processor and system to handle only one security level at a time.

single-use passwords

A variant of dynamic passwords that are changed every time they are used.

Skipjack

Associated with the Escrowed Encryption Standard, an algorithm that operates on 64-bit blocks of text. It uses an 80-bit key and supports the same four modes of operation supported by DES. Skipjack was proposed but never implemented by the U.S. government. It provides the cryptographic routines supporting the Clipper and Capstone high-speed encryption chips designed for mainstream commercial use.

smart card

Credit-card-sized ID, badge, or security pass that has a magnetic strip, bar code, or integrated circuit chip embedded in it. Smart cards can contain information about the authorized bearer that can be used for identification and/or authentication purposes.

smurf attack

A type of DoS. A smurf attack occurs when an amplifying server or network is used to flood a victim with useless data.

sniffer attack

Any activity that results in a malicious user obtaining information about a network or the traffic over that network. A sniffer is often a packet-capturing program that duplicates the contents of packets traveling over the network medium into a file. Also referred to as a snooping attack.

sniffing

A form of network traffic monitoring. Sniffing often involves the capture or duplication of network traffic for examination, re-creation, and extraction.

snooping attack

See *sniffer attack*.

social engineering

A skill by which an unauthorized person gains the trust of someone inside your organization and encourages them to make a change to the IT system in order to grant them access.

socket

Another name for a port.

software IP encryption (SWIPE)

A layer 3 security protocol for IP. It provides authentication, integrity, and confidentiality using an encapsulation protocol.

spam

The term describing unwanted email, newsgroup, or discussion forum messages. Spam can be as innocuous as an advertisement from a well-meaning vendor or as malignant as floods of unrequested messages with viruses or Trojan horses attached.

spamming attacks

Sending significant amounts of spam to a system in order to cause a DoS or general irritation, consume storage space, or consume bandwidth and processing capabilities.

spike

Momentary high voltage.

split knowledge

The specific application of the ideas of separation of duties and two-man control into a single solution. The basic idea is that the information or privilege required to perform an operation is divided among multiple users. This ensures that no single person has sufficient privileges to compromise the security of the environment.

spoofing

The act of replacing the valid source and/or destination IP address and node numbers with false ones.

spoofing attack

Any attack that involves spoofed or modified packets.

standards

Documents that define compulsory requirements for the homogenous use of hardware, software, technology, and security controls. They provide a course of action by which technology and procedures are uniformly implemented throughout an organization. Standards are tactical documents that define steps or methods to accomplish the goals and overall direction defined by security policies.

state

A snapshot of a system at a specific instance in time.

state machine model

A system that is designed so that no matter what function is performed, it is always a secure system.

stateful inspection firewall

A firewall that evaluates the state or the context of network traffic. By examining source and destination address, application usage, source of origin, and relationship between current packets with the previous packets of the same session, stateful inspection firewalls are able to grant a broader range of access for authorized users and activities and actively watch for and block unauthorized users and activities. Stateful inspection firewalls are known as third-generation firewalls.

static packet-filtering firewall

A firewall that filters traffic by examining data from a message header. Usually the rules are concerned with source, destination, and port addresses. Static packet-filtering firewalls as known as first-generation firewalls.

static password

Password that does not change over time or that remains the same for a significant period of time.

static token

A physical means to provide identity, usually not employed as an authentication factor. Examples include a swipe card, a smart card, a floppy disk, a USB RAM dongle, or even something as simple as a key to operate a physical lock.

station set identifier (SSID)

The name of a wireless network that each wireless client must know in order to communicate with the host access point.

statistical attack

This type of attack exploits statistical weaknesses in a cryptosystem, such as such as floating-point errors or an inability to produce random numbers. It attempts to find vulnerabilities in the hardware or operating system hosting the cryptography application.

statistical intrusion detection

See *behavior-based detection*.

stealth virus

A virus that hides itself by actually tampering with the operating system to fool antivirus packages into thinking that everything is functioning normally.

steganography

The act of embedding messages within another message, commonly used within an image or a WAV file.

stop error

The security response of an operating system, such as Windows, when an application performs an illegal operation, such as accessing hardware or modifying/accessing the memory space of another process.

stopped state

The state in which a process is finished or must be terminated. At this point, the operating system can recover all memory and other resources allocated to the process and reuse them for other processes as needed.

strategic plan

A long-term plan that is fairly stable. It defines the organization's goals, mission, and objectives. A strategic plan is useful for about five years if it is maintained and updated annually. The strategic plan also serves as the planning horizon.

stream attack

A type of DoS. A stream attack occurs when a large number of packets are sent to numerous ports on the victim system using random source and sequence numbers. The processing performed by the victim system attempting to make sense of the data will result in a DoS. Also referred to as flooding.

stream ciphers

Ciphers that operate on each character or bit of a message (or data stream) one character/bit at a time.

strong password

Password that is resistant to dictionary and brute-force attacks.

Structured Query Language (SQL)

The standard language used by relational databases to enter and extract the information stored in them.

structured walk-through

A type of disaster recovery test, often referred to as a “table-top exercise,” in which members of the disaster recovery team gather in a large conference room and role-play a disaster scenario.

subject

An active entity that seeks information about or data from passive objects through the exercise of access. A subject can be a user, a program, a process, a file, a computer, a database, and so on.

subpoena

A court order that compels an individual or organization to surrender evidence or to appear in court.

substitution cipher

Cipher that uses an encryption algorithm to replace each character or bit of the plain-text message with a different character, such as a Caesar cipher.

supervisor state (or supervisory state)

The state in which a process is operating in a privileged, all-access mode.

supervisory mode

Mode in which processes at layer 0 run, which is the ring where the operating system itself resides.

surge

Prolonged high voltage.

SWIPE

See *software IP encryption (SWIPE)*.

switch

A network device that is an intelligent hub because it knows the addresses of the systems connected on each outbound port. Instead of repeating traffic on every outbound port, a switch repeats only traffic out of the port on which the destination is known to exist. Switches offer greater efficiency for traffic delivery, create separate broadcast and collision domains, and improve the overall throughput of data.

Switched Multimegabit Data Services (SMDS)

A connectionless network communication service. SMDS provides bandwidth on demand. SMDS is a preferred connection mechanism for linking remote LANs that communicate infrequently.

switched virtual circuit (SVC)

A virtual circuit that must be rebuilt each time it is used; similar to a dial-up connection.

semantic integrity mechanisms

A common security feature of a DBMS. This feature ensures that no structural or semantic rules are violated. It also checks that all stored data types are within valid domain ranges, that only logical values exist, and that any and all uniqueness constraints are met.

symmetric key

An algorithm that relies upon a “shared secret” encryption key that is distributed to all members who participate in communications. This key is used by all parties to both encrypt and decrypt messages.

symmetric multiprocessing (SMP)

A type of system in which the processors share not only a common operating system but also a common data bus and memory resources. In this type of arrangement, it is not normally possible to use more than 16 processors.

SYN flood attack

A type of DoS. A SYN flood attack is waged by not sending the final ACK packet, which breaks the standard three-way handshake used by TCP/IP to initiate communication sessions.

Synchronous Data Link Control (SDLC)

A layer 2 protocol employed by networks with dedicated or leased lines. SDLC was developed by IBM for remote communications with SNA systems. SDLC is a bit-oriented synchronous protocol.

synchronous dynamic password token

Tokens used in a token device that generates passwords at fixed time intervals. Time interval tokens require that the clock of the authentication server and the token device be synchronized. The generated password is entered by the subject along with a PIN, passphrase, or password.

system call

A process by which an object in a less-trusted protection ring requests access to resources or functionality by objects in more-trusted protection rings.

system high mode

See *system-high security mode*.

system-high security mode

Mode in which systems are authorized to process only information that all system users are cleared to read and have a valid need to know. Systems running in this mode are not trusted to maintain separation between security levels, and all information processed by these systems must be handled as if it were classified at the same level as the most highly classified information processed by the system.

T

table

The main building block of a relational database; also known as a relation.

TACACS

See *Terminal Access Controller Access Control System (TACACS)*.

tactical plan

A midterm plan developed to provide more details on accomplishing the goals set forth in the strategic plan. A tactical plan is typically useful for about a year. It often prescribes and schedules the tasks necessary to accomplish organizational goals.

Take-Grant model

A model that employs a directed graph to dictate how rights can be passed from one subject to another or from a subject to an object. Simply put, a subject with the grant right can grant another subject or another object any other right they possess. Likewise, a subject with the take right can take a right from another subject.

task-based

An access control methodology in which access is granted based on work tasks or operations.

TCP wrapper

An application that can serve as a basic firewall by restricting access based on user IDs or systems IDs.

teardrop attack

A type of DoS. A teardrop attack occurs when an attacker exploits a bug in operating systems. The bug exists in the routines used to reassemble fragmented packets. An attacker sends numerous specially formatted fragmented packets to the victim, which causes the system to freeze or crash.

technical access control

The hardware or software mechanisms used to manage access to resources and systems and provide protection for those resources and systems. Examples of logical or technical access controls include encryption, smart cards, passwords, biometrics, constrained interfaces, access control lists, protocols, firewalls, routers, IDEs, and clipping levels. The same as logical access control.

technical physical security controls

Security controls that use technology to implement some form of physical security, including intrusion detection systems, alarms, CCTV, monitoring, HVAC, power supplies, and fire detection and suppression.

TEMPEST

The study and control of electronic signals produced by various types of electronic hardware, such as computers, televisions, phones, and so on. Its primary goal is to prevent EM and RF radiation from leaving a strictly defined area so as to eliminate the possibility of external radiation monitoring, eavesdropping, and signal sniffing.

Terminal Access Controller Access Control System (TACACS)

An alternative to RADIUS. TACACS is available in three versions: original TACACS, XTACACS (extended TACACS), and TACACS+. TACACS integrates the authentication and authorization processes. XTACACS keeps the authentication, authorization, and accounting processes separate. TACACS+ improves XTACACS by adding two-factor authentication.

terrorist attacks

Attacks that differ from military and intelligence attacks in that the purpose is to disrupt normal life, whereas a military or intelligence attack is designed to extract secret information.

test data method

A form of program testing that examines the extent of the system testing to locate untested program logic.

testimonial evidence

Evidence that consists of the testimony of a witness, either verbal testimony in court or written testimony in a recorded deposition.

thicknet

See *10Base5*.

thin client

A term used to describe a workstation that has little or no local processing or storage capacity. A thin client is used to connect to and operate a remote system.

thinnet

See *10Base2*.

threat

A potential occurrence that may cause an undesirable or unwanted outcome for an organization or a specific asset.

threat agents

People, programs, hardware, or systems that intentionally exploit vulnerabilities.

threat events

Accidental exploitations of vulnerabilities.

thrill attacks

An attack launched by crackers with few true skills. The main motivation behind thrill attacks is the “high” of getting into a system.

throughput rate

The rate at which a biometric device can scan and authenticate subjects. A rate of about six seconds or faster is required for general acceptance of a specific biometric control.

ticket

An electronic authentication factor used by the Kerberos authentication system.

ticket-granting service (TGS)

An element of the Kerberos authentication system. The TGS manages the assignment and expiration of tickets. Tickets are used by subjects to gain access to objects.

time-of-check (TOC)

The time at which a subject checks on the status of an object.

time-of-check-to-time-of-use (TOCTTOU)

A timing vulnerability that occurs when a program checks access permissions too far in advance of a resource request.

time-of-use (TOU)

The time at which the decision is made by a subject to access an object.

time slice

A single chunk or division of processing time.

token

See *token device*.

token device

A password-generating device that subjects must carry with them. Token devices are a form of a “something you have” (Type 2) authentication factor.

token ring

A token-passing LAN technology.

Top Secret

The highest level of government/military classification. Unauthorized disclosure of top-secret data will cause exceptionally grave damage to national security.

topology

The physical layout of network devices and connective cabling. The common network topologies are ring, bus, star, and mesh.

total risk

The amount of risk an organization would face if no safeguards were implemented. Threats * vulnerabilities * asset value = total risk.

trade secret

Intellectual property that is absolutely critical to a business and would cause significant damage if it were disclosed to competitors and/or the public.

trademark

A registered word, slogan, or logos used to identify a company and its products or services.

traffic analysis

A form of monitoring in which the flow of packets rather than the actual content of packets is examined. Also referred to as trend analysis.

training

The task of teaching employees to perform their work tasks and to comply with the security policy. All new employees require some level of training so they will be able to properly comply with all standards, guidelines, and procedures mandated by the security policy.

transferring risk

Placing the cost of loss from a realized risk onto another entity or organization, such as purchasing insurance. Also referred to as assigning risk.

transient

A short duration of line noise disturbance.

Transmission Control Protocol (TCP)

A connection-oriented protocol located at layer 4 of the OSI model.

transmission error correction

A capability built into connection- or session-oriented protocols and services. If it is determined that a message, in whole or in part, was corrupted, altered, or lost, a request can be made for the source to resend all or part of the message.

transmission logging

A form of auditing focused on communications. Transmission logging records the details about source, destination, time stamps, identification codes, transmission status, number of packets, size of message, and so on.

transparency

A characteristic of a service, security control, or access mechanism that is unseen by users. Transparency is often a desirable feature for security controls.

Transport layer

Layer 4 of the OSI model.

transport mode

A mode of IPSec when used in a VPN. In transport mode, the IP packet data is encrypted, but the header of the packet is not.

transposition cipher

Cipher that uses an encryption algorithm to rearrange the letters of a plain-text message to form the cipher-text message.

trap door

Undocumented command sequence that allows software developers to bypass normal access restrictions.

traverse mode noise

EMI noise generated by the difference in power between the hot and neutral wires of a power source or operating electrical equipment.

trend analysis

See *traffic analysis*.

Triple DES (3DES)

A standard that uses three iterations of DES with two or three different keys to increase the effective key strength to 112 bits.

Trojan horse

A malicious code object that appears to be a benevolent program—such as a game or simple utility that performs the “cover” functions as advertised but also carries an unknown payload, such as a virus.

trust

A security bridge established to share resources from one domain to another. A trust is established between two domains to allow users from one domain to access resources in another. Trusts can be one-way only, or they can be two-way.

trusted computing base (TCB)

The combination of hardware, software, and controls that form a trusted base that enforces your security policy.

trusted path

Secure channel used by the TCB to communicate with the rest of the system.

trusted recovery process

On a secured system, a process that ensures the system always returns to a secure state after an error, failure, or reboot.

trusted system

A secured computer system.

tunnel mode

A mode of IPSec when used in a VPN. In tunnel mode, the entire IP packet is encrypted and a new header is added to the packet to govern transmission through the tunnel.

tunneling

A network communications process that protects the contents of protocol packets by encapsulating them in packets of another protocol.

turnstile

A form of gate that prevents more than one person at a time from gaining entry and often restricts movement in one direction.

twisted-pair

See *10Base-T*.

two-factor authentication

Authentication that requires two factors.

Type 1 authentication factor

Something you know, such as a password, personal identification number (PIN), combination lock, passphrase, mother's maiden name, or favorite color.

Type 2 authentication factor

Something you have, such as a smart card, ATM card, token device, or memory card.

Type 3 authentication factor

Something you are, such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, or hand geometry.

Type 1 error

See *false rejection rate (FRR)*.

Type 2 error

See *false acceptance rate (FAR)*.

U

unclassified

The lowest level of government/military classification. Used for data that is neither sensitive nor classified. Disclosure of unclassified data does not compromise confidentiality, and it doesn't cause any noticeable damage.

unicast

A communications transmission to a single identified recipient.

Uniform Computer Information Transactions Act (UCITA)

A federal law designed for adoption by each of the 50 states to provide a common framework for the conduct of computer-related business transactions.

uninterruptible power supply (UPS)

A type of self-charging battery that can be used to supply consistent clean power to sensitive equipment. A UPS functions basically by taking power in from the wall outlet, storing it in a battery, pulling power out of the battery, and then feeding that power to whatever devices are connected to it. By directing current through its battery, it is able to maintain a consistent clean power supply.

unit testing

A method of testing software. Each unit of code is tested independently to discover any errors or omissions and to ensure that it functions properly. Unit testing should be performed by the development staff.

unshielded twisted-pair (UTP)

A twisted-pair wire that does not include additional EMI protection. Most twisted-pair wiring is UTP.

upper management

See *senior management*.

USA Patriot Act of 2001

An act implemented after the September 11, 2001, terrorist attacks. It greatly broadened the powers of law enforcement organizations and intelligence agencies across a number of areas, including the monitoring of electronic communications.

user

Any person who has access to the secured system. A user's access is tied to their work tasks and is limited so they have only enough access to perform the tasks necessary for their job position (in other words, principle of least privilege). Also referred to as an end user and employee.

User Datagram Protocol (UDP)

A connectionless protocol located at layer 4 of the OSI model.

user mode

The basic mode used by the CPU when executing user applications.

V

VENONA

One of the major intelligence successes of the United States resulted when cryptanalysts broke a top-secret Soviet cryptosystem, i.e., VENONA, that relied upon the use of one-time pads

Vernam cipher

A device that implements a 26-character modulo 26 substitution cipher. It functions as a one-time pad.

view

A client interface used to interact with a database. The view limits what clients can see and what functions they can perform.

Vigenere cipher

A polyalphabetic substitution cipher.

violation analysis

A form of auditing that uses clipping levels.

virtual machine

A software simulation of a computer within which a process executes. Each virtual machine has its own memory address space and communication between virtual machines is securely controlled.

virtual memory

A special type of secondary memory that is managed by the operating system in such a manner that it appears to be real memory.

virtual private network (VPN)

A network connection established between two systems over an existing private or public network. A VPN provides confidentiality and integrity for network traffic through the use of encryption.

virtual private network (VPN) protocol

The protocols, such as PPTP, L2TP, and IPSec, that are used to create VPNs.

virus

The oldest form of malicious code objects that plague cyberspace. Once they are in a system, they attach themselves to legitimate operating system and user files and applications and normally perform some sort of undesirable action, ranging from the somewhat innocuous display of an annoying message on the screen to the more malicious destruction of the entire local file system.

Voice over IP (VoIP)

A network service that provides voice communication services by transporting the voice traffic as network packets over an IP network.

voice pattern

An example of a biometric factor, which is a behavioral or physiological characteristic that is unique to a subject. The speech, tone, modulation, and pitch patterns of a person's voice are used to establish identity or provide authentication.

volatile

See *volatile storage*.

volatile storage

A storage medium, such as RAM, that loses its contents when power is removed from the resource.

voluntarily surrender

The act of willingly handing over evidence.

vulnerability

The absence or weakness of a safeguard or countermeasure. In other words, a vulnerability is the existence of a flaw, loophole, oversight, error, limitation, frailty, or susceptibility in the IT infrastructure or any other aspect of an organization.

vulnerability scan

A test performed on a system to find weaknesses in the security infrastructure.

vulnerability scanner

A tool used to test a system for known security vulnerabilities and weaknesses. Vulnerability scanners are used to generate reports that indicate the areas or aspects of the system that need to be managed to improve security.

W

wait state

The state in which a process is ready to execute but is waiting for an operation such as keyboard input, printing, or file writing to complete.

war dialing

The act of using a modem to search for a system that will accept inbound connection attempts.

warm site

A middle ground between hot sites and cold sites for disaster recovery specialists. A warm site always contains the equipment and data circuits necessary to rapidly establish operations but does not typically contain copies of the client's data.

warning banners

Messages used to inform would-be intruders or attempted security policy violators that their intended activities are restricted and that any further activities will be audited and monitored. A warning banner is basically an electronic equivalent of a no trespassing sign.

well-known ports

The first 1,024 ports of TCP and UDP. They are usually assigned to commonly used services and applications.

wet pipe system

A fire suppression system that is always full of water. Water discharges immediately when triggered by a fire or smoke. Also known as a closed head system.

white box testing

A form of program testing that examines the internal logical structures of a program.

wide area network (WAN)

A network or a network of LANs that is geographically diverse. Often dedicated leased lines are used to establish connections between distant components.

WiFi Protected Access (WPA)

An early alternative to WEP based on a secret passphrase and employing the LEAP and TKIP crypto systems. It is attackable through passphrase guessing.

WiMax (802.16)

A wireless standard that defines citywide wireless access technologies. This standard has yet to be widely deployed.

WinNuke attack

A type of DoS. A WinNuke attack is a specialized assault against Windows 95 systems. Out-of-band TCP data is sent to a victim's system, which causes the OS to freeze.

Wired Equivalent Privacy (WEP)

A form of encrypted authentication that employs RC4. WEP supports only one-way authentication from client to WAP. WEP is considered insufficient for security because of several deficiencies in its design and implementation.

Wireless Application Protocol (WAP)

A functioning industry-driven protocol stack that allows users through their WAP-capable devices, such as cell phones, to communicate over a carrier's network with the Internet.

wireless networking (802.11)

A form of networking that uses radio waves as the connection medium following the 802.11 standard. Often called WiFi.

work function or work factor

A way of measuring the strength of a cryptography system by measuring the effort in terms of cost and/or time. Usually the time and effort required to perform a complete brute-force attack against an encryption system is what the work function rating represents. The security and protection offered by a cryptosystem is directly proportional to the value of the work function/factor.

worm

A form of malicious code that is self-replicating but is not designed to impose direct harm on host systems. The primary purpose of a worm is to replicate itself to other systems and gather information. Worms are usually very prolific and often cause a denial of service because of their consumption of system resources and network bandwidth in their attempt to self-replicate.

X

X.25

An older WAN protocol that uses carrier switching to provide end-to-end connections over a shared network medium.

XOR

A function that returns a true value when only one of the input values is true. If both values are false or both values are true, the output of the XOR function is false.

Z

zero knowledge proof

A concept of communication whereby a specific type of information is exchanged but no real data is exchanged. Great examples of this idea are digital signatures and digital certificates.

Zero Knowledge Teams

These possess only primary information about an organization during a security assessment or penetration test.