

Physical Security

If someone really wants to get at the information, it is not difficult if they can gain physical access to the computer or hard drive.

MICROSOFT WHITE PAPER, JULY 1999

Amy Windahl was back early from lunch. As she was walking toward the SLS building from the parking lot, she saw one of the accounting clerks go through the building's double glass doors. Behind him followed someone she didn't recognize, a tall, blond man in nondescript business casual clothes. The two of them walked past the lobby security guard and headed for the elevators. Amy got on the next elevator and pressed the button for her floor.

When the elevator doors opened, she saw the blond man in the second floor elevator lobby looking at the company's phone list. She walked over to the secure doors that led to the offices and cocked her right hip, where her badge was clipped, toward the sensor for the locks. When she heard the electric lock release, Amy went through. As the door began to shut, the stranger grabbed it and came through behind her.

Amy knew now that he was a *tailgater*, a person who follows authorized people after they have used their badges to open locked doors. Just last week a security bulletin had emphasized that tailgaters should be reported. Everyone in the staff meeting joked about turning each other in the next time any two of them came through the door together. But now she was beginning to understand the seriousness of the bulletin.

Amy went back to the second floor lobby and used the phone there to call building security and report the tailgater.

“Do you guys want to check it out?”

“Yes, ma’am. We have someone nearby. I’ll have him meet you in the lobby,” said the security dispatcher.

When the security officer arrived, Amy described the man, and said, “He went down the hall, toward the programming offices.”

The guard said, “Wait here. If he comes through here again, call dispatch at extension 3333. I’ll be right back.”

A few minutes later, Amy saw the blond man walking briskly toward the doors; the guard was right behind him. As the stranger opened the door, the guard called out, “Sir, please stop. I need to speak with you. What’s your name?” Before the blond man could answer, the elevator opened, and two more guards came into the lobby.

The stranger said, “Alan Gaskin.”

The guard asked, “What’s your business here?”

“Just visiting a friend,” said the man.

“And who would that be?” the guard asked.

The stranger looked a bit surprised, and then said, “Uh, William Walters, in the accounting department, I think.”

The guard reached for his PDA and punched a few buttons. Then he said, “Mr. Gaskin, there are no employees with that name working here, in accounting or any other department. Do you want to try another answer?”

The intruder took a few steps toward the stairwell, but the other two guards moved up and cut him off. As they held the man’s arms to keep him from escaping, a brown paper bag dropped out from under his jacket, its contents spilling out on the carpet. Amy saw several office badges, a watch, two small tablet computers and several cell phones.

The first guard radioed dispatch. “Contact the local police and advise them we have a thief and we plan to press charges.” The other guards led the man toward the elevators, while the first guard told Amy: “Call your supervisor and tell her you’ll be delayed. We need a statement from you.”

LEARNING OBJECTIVES:

Upon completion of this material, you should be able to:

- Discuss the relationship between information security and physical security
- Describe key physical security considerations, including fire control and surveillance systems
- Identify critical physical environment considerations for computing facilities, including uninterruptible power supplies

Introduction

As you learned in Chapter 1, information security requires the protection of both data and physical assets. You have already learned about many of the mechanisms used to protect data, including firewalls, intrusion detection systems, and monitoring software.

Physical security encompasses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization, including the people, hardware, and supporting system elements and resources that control information in all its states (transmission, storage, and processing). Most technology-based controls can be circumvented if an attacker gains physical access to the devices being controlled. In other words, if it is easy to steal the hard drives from a computer system, then the information on those hard drives is not secure. Therefore, physical security is just as important as logical security to an information security program.

In earlier chapters, you encountered a number of threats to information security that could be classified as threats to physical security. For example, an employee accidentally spilling coffee on a laptop threatens the physical security of the information in the computer—in this case, the threat is an act of human error or failure. A compromise to intellectual property can include an employee without an appropriate security clearance copying a classified marketing plan. A deliberate act of espionage or trespass could be a competitor sneaking into a facility with a camera. Deliberate acts of sabotage or vandalism can be physical attacks on individuals or property. Deliberate acts of theft include employees stealing computer equipment, credentials, passwords, and laptops. Quality of service deviations from service providers, especially power and water, also represent physical security threats, as do various environmental anomalies. In his book, *Fighting Computer Crime*, Donn B. Parker lists the following “Seven Major Sources of Physical Loss”:

1. Extreme temperature: heat, cold
2. Gases: war gases, commercial vapors, humid or dry air, suspended particles
3. Liquids: water, chemicals
4. Living organisms: viruses, bacteria, people, animals, insects
5. Projectiles: tangible objects in motion, powered objects
6. Movement: collapse, shearing, shaking, vibration, liquefaction, flow waves, separation, slide
7. Energy anomalies: electrical surge or failure, magnetism, static electricity, aging circuitry; radiation: sound, light, radio, microwave, electromagnetic, atomic¹

As with all other areas of security, the implementation of physical security measures requires sound organizational policy. Physical security policies guide users on the appropriate use of computing resources and information assets, as well as on the protection of their own personal safety in day-to-day operations. Physical security is designed and implemented in several layers. Each of the organization’s communities of interest is responsible for components within these layers, as follows:

- General management is responsible for the security of the facility in which the organization is housed and the policies and standards for secure operation. This includes



exterior security, fire protection, and building access, as well as other controls such as guard dogs and door locks.

- IT management and professionals are responsible for environmental and access security in technology equipment locations, and for the policies and standards that govern secure equipment operation. This includes access to server rooms, and power conditioning and server room temperature and humidity controls, and more specialized controls like static and dust contamination equipment.
- Information security management and professionals are responsible for risk assessments and for reviewing the physical security controls implemented by the other two groups.

Physical Access Controls

A number of physical access controls are uniquely suited to governing the movement of people within an organization's facilities—specifically, controlling their physical access to company resources. While logical access to systems, in this age of the Internet, is a very important subject, the control of physical access to the assets of the organization is also of critical importance. Some of the technology used to control physical access is also used to control logical access, including biometrics, smart cards, and wireless enabled keycards.

Before learning more about physical access controls, you need to understand what makes a facility secure. An organization's general management oversees its physical security. Commonly, a building's access controls are operated by a group called **facilities management**. Larger organizations may have an entire staff dedicated to facilities management, while smaller organizations often outsource these duties.

In facilities management, a **secure facility** is a physical location that has in place controls to minimize the risk of attacks from physical threats. The term *secure facility* might bring to mind military bases, maximum-security prisons, and nuclear power plants, but while securing a facility requires some adherence to rules and procedures, the environment does not necessarily have to be that constrained. It is also not necessary that a facility resemble a fortress to minimize risk from physical attacks. In fact, a secure facility can sometimes use its natural terrain, local traffic flow, and surrounding development to enhance its physical security, along with protection mechanisms such as fences, gates, walls, guards, and alarms.

Physical Security Controls

There are a number of physical security controls that an organization's communities of interest should consider when implementing physical security inside and outside the facility. Some of the major controls are:

- Walls, fencing, and gates
- Guards
- Dogs
- ID cards and badges
- Locks and keys

- Mantraps
- Electronic monitoring
- Alarms and alarm systems
- Computer rooms and wiring closets
- Interior walls and doors

Walls, Fencing, and Gates Some of the oldest and most reliable elements of physical security are walls, fencing, and gates. While not every organization needs to implement external perimeter controls, walls and fences with suitable gates are an essential starting point for organizations whose employees require access to physical locations the organization owns or controls. These types of controls vary widely in appearance and function, ranging from chain link or privacy fences that control where people should park or walk, to imposing concrete or masonry barriers designed to withstand the blast of a car bomb. Each exterior perimeter control requires expert planning to ensure that it fulfills the security goals and that it presents an image appropriate to the organization.

Guards Controls like fences and walls with gates are static, and are therefore unresponsive to actions, unless they are programmed to respond with specific actions to specific stimuli, such as opening for someone who has the correct key. Guards, on the other hand, can evaluate each situation as it arises and make reasoned responses. Most guards have clear **standard operating procedures (SOPs)** that help them to act decisively in unfamiliar situations. In the military, for example, guards are given general orders (see the Offline on guard duty), as well as special orders that are particular to their posts.

Dogs If an organization is protecting valuable resources, dogs can be a valuable part of physical security if they are integrated into the plan and managed properly. Guard dogs are useful because their keen sense of smell and hearing can detect intrusions that human guards cannot, and they can be placed in harm's way when necessary to avoid risking the life of a person.

ID Cards and Badges An **identification (ID) card** is typically concealed, whereas a **name badge** is visible. Both devices can serve a number of purposes. First, they serve as simple forms of biometrics in that they use the cardholder's picture to authenticate his or her access to the facility. The cards may be visibly coded to specify which buildings or areas may be accessed. Second, ID cards that have a magnetic strip or radio chip that can be read by automated control devices allow an organization to restrict access to sensitive areas within the facility. ID cards and name badges are not foolproof, however; and even the cards designed to communicate with locks can be easily duplicated, stolen, or modified. Because of this inherent weakness, such devices should not be an organization's only means of controlling access to restricted areas.

Another inherent weakness of this type of physical access control technology is the human factor. As depicted in this chapter's opening vignette, **tailgating** occurs when an authorized person presents a key to open a door, and other people, who may or may not be authorized, also enter. Launching a campaign to make employees aware of tailgating is one way to combat this problem. There are also technological means of discouraging tailgating, such as





Offline Guard Duty

“General Orders:

I will guard everything within the limits of my post and quit my post only when properly relieved.

I will obey my special orders and perform all of my duties in a military manner.

I will report violations of my special orders, emergencies, and anything not covered in my instructions to the commander of the relief.”²

How do guards meet these responsibilities? They apply the force necessary to accomplish their missions, including deadly force in approved situations. Deadly force is the application of coercive control that may result in death or severe bodily harm. It is applied only to the extent necessary to make an apprehension.

“Deadly force can only be used for [the following situations]:

1. Self-defense in the event of imminent danger of death or serious bodily harm;
2. To prevent the actual theft or destruction of property designated for protection; and
3. As directed by the Standard Operating Procedures of his individual guard post.”³

Adapted from “Guard Duty,” www.armystudyguide.com/content/army_board_study_guide_topics/guard_duty/guard-duty-study-guide.shtml. In the military, guard duty is a serious responsibility. A guard must memorize, understand, and comply with his or her general orders, and the orders particular to his or her assignment.

mantraps (which are discussed in a following section) or turnstiles. These extra levels of control are usually expensive, in that they require floor space and/or construction, and are inconvenient for those required to use them. Consequently, anti-tailgating controls are only used where there is significant security risk from unauthorized entry.

Locks and Keys There are two types of lock mechanisms: mechanical and electromechanical. The **mechanical lock** may rely on a key that is a carefully shaped piece of metal, which is rotated to turn tumblers that release secured loops of steel, aluminum, or brass (as in, for example, brass padlocks). Alternatively, a mechanical lock may have a dial that rotates slotted discs until the slots on multiple disks are aligned, and then retracts a securing bolt (as in combination and safe locks). Although mechanical locks are conceptually simple, some of the technologies that go into their development are quite complex. Some of these modern enhancements have led to the creation of the electromechanical lock. **Electromechanical locks** can accept a variety of inputs as keys, including magnetic strips on ID cards, radio signals from name badges, personal identification numbers (**PINs**) typed into a keypad, or some combination of these to activate an electrically powered locking mechanism.

Locks can also be divided into four categories based on the triggering process: manual, programmable, electronic, and biometric. **Manual locks** such as padlocks and combination

locks, are commonplace and well understood. If you have the key (or combination) you can open the lock. These locks are often preset by the manufacturer and therefore unchangeable. In other words, once manual locks are installed into doors, they can only be changed by highly trained locksmiths. Programmable locks can be changed after they are put in service, allowing for combination or key changes without a locksmith and even allowing the owner to change to another access method (key or combination) to upgrade security. Many examples of these types of locks are shown in Figure 9-1. Mechanical push button locks, shown in the left-most photo in Figure 9-1, are popular for securing computer rooms and wiring closets, as they have a code that can be reset and don't require electricity to operate.

Electronic locks can be integrated into alarm systems and combined with other building management systems. Also, these locks can be integrated with sensors to create various combinations of locking behavior. One such combination is a system that coordinates the use of fire alarms and locks to improve safety during alarm conditions (i.e., fires). Such a system changes a location's required level of access authorization when that location is in an alarm condition. Another example is a combination system in which a lock is fitted with a sensor that notifies guard stations when that lock has been activated. Another common form of electronic locks are electric strike locks, which usually require people to announce themselves before being "buzzed" through a locked door. In general, electronic locks lend themselves to uses where they can be activated or deactivated by a switch controlled by an agent, usually a secretary or guard. Electronic push button locks, like their mechanical cousins, have a numerical keypad over the knob, requiring the individual user to enter a personal code and open the door. These locks usually use battery backups to power the keypad in case of a power failure.

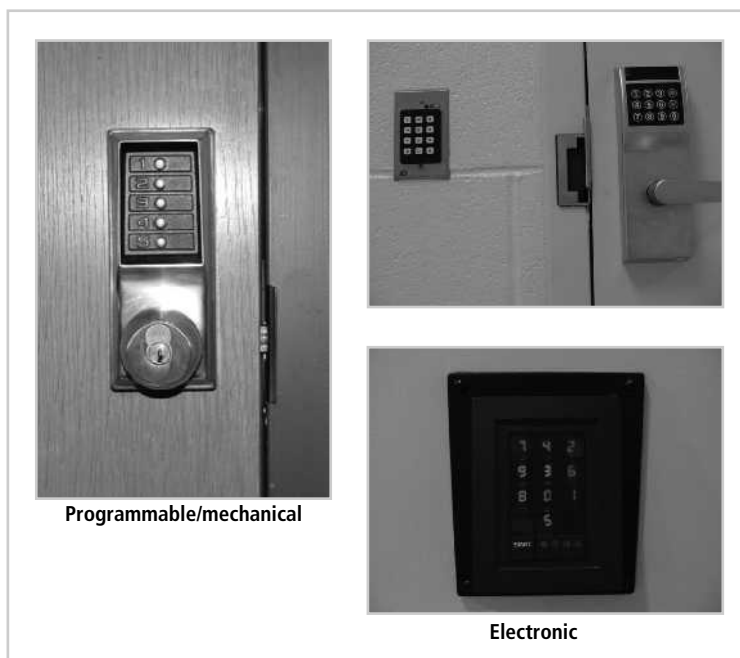


Figure 9-1 Locks

Source: Course Technology/Cengage Learning

Some locks use smart cards, as described previously—keys that contain computer chips. These smart cards can carry critical information, provide strong authentication, and offer a number of other features. Keycard readers based on smart cards are often used to secure computer rooms, communications closets, and other restricted areas. The card reader can track entry and provide accountability. In a locking system that uses smart cards, the access level of individuals can be adjusted according to their current status (i.e., current employee, recently resigned) and thus personnel changes do not require replacement of the lock. A specialized type of keycard reader is the **proximity reader**, which, instead of requiring individuals to insert their cards, allows them simply to place their cards within the reader's range. Some of these readers can recognize the card even when it is inside a pocket.

The most sophisticated locks are **biometric locks**. Finger, palm, and hand readers, iris and retina scanners, and voice and signature readers fall into this category. The technology that underlies biometric devices is discussed in Chapter 7.

The management of keys and locks is fundamental to the fulfillment of general management's responsibility to secure an organization's physical environment. As you will learn in Chapter 11, when people are hired, fired, laid off, or transferred, their access controls, whether physical or logical, must be appropriately adjusted. Failure to do so can result in employees cleaning out their offices and taking more than their personal effects. Also, when locksmiths are hired, they should be carefully screened and monitored, as there is a chance that they could have complete access to the facility.

Sometimes locks fail, and thus facilities need to have alternative procedures in place for controlling access. These procedures must take into account that locks fail in one of two ways: the door lock fails and the door becomes unlocked—a **fail-safe lock**; or the door lock fails and the door remains locked—a **fail-secure lock**. In practice, the most common reason why technically sophisticated locks fail is loss of power and activation through fire control systems. A fail-safe lock is usually used to secure an exit, where it is essential that in the event of, for instance, a fire, the door is unlocked. A fail-secure lock is used when human safety in the area being controlled is not the dominant factor. One example of this is a situation in which the security of nuclear or biological weapons needs to be controlled; here, preventing a loss of control of these weapons is more critical to security (meaning it is a security issue of greater magnitude) than protecting the lives of the personnel guarding the weapons.

Understanding lock mechanisms is important, because locks can be exploited by an intruder to gain access to the secured location. If an electronic lock is short circuited, it may become fail-safe and allow the intruder to bypass the control and enter the room.

Mantraps A common enhancement for locks in high security areas is the mantrap. A **mantrap** is a small enclosure that has separate entry and exit points. To gain access to the facility, area, or room, a person enters the mantrap, requests access via some form of electronic or biometric lock and key, and if confirmed, exits the mantrap into the facility. Otherwise the person cannot leave the mantrap until a security official overrides the enclosure's automatic locks. Figure 9-2 provides an example of a typical mantrap layout.

Electronic Monitoring Monitoring equipment can be used to record events within a specific area that guards and dogs might miss, or in areas where other types of physical controls are not practical. Although you may not know it, many of you are, thanks to the silver globes attached to the ceilings of many retail stores, already subject to cameras viewing you

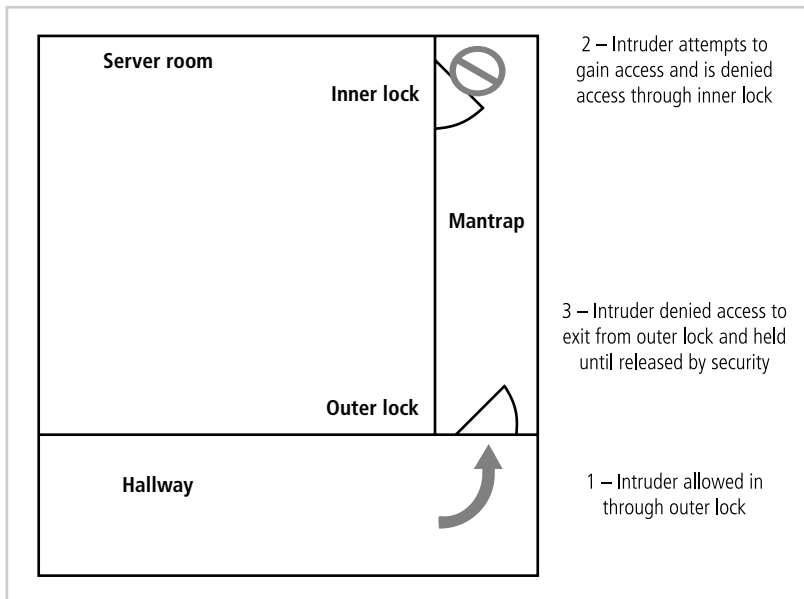


Figure 9-2 Mantraps

Source: *Course Technology/Cengage Learning*



from odd corners—that is, video monitoring. Attached to these cameras are video cassette recorders (VCRs) and related machinery that capture the video feed. Electronic monitoring includes **closed-circuit television (CCT)** systems. Some CCT systems collect constant video feeds, while others rotate input from a number of cameras, sampling each area in turn.

These video monitoring systems have drawbacks: for the most part they are passive and do not prevent access or prohibited activity. Another drawback to these systems is that people must view the video output, because there are no intelligent systems capable of reliably evaluating a video feed. To determine if unauthorized activities have occurred, a security staff member must constantly review the information in real time or review the information collected in video recordings. For this reason, CCT is most often used as an evidence collection device after an area has been broken into than as a detection instrument. In high-security areas (such as banks, casinos, and shopping centers), however, security personnel monitor CCT systems constantly, looking for suspicious activity.

Alarms and Alarm Systems Closely related to monitoring are the alarm systems that notify people or systems when a predetermined event or activity occurs. Alarms, which are similar to the IDPSs you learned about in Chapter 7, can detect a *physical* intrusion or other untoward event. This could be a fire, a break-in, an environmental disturbance such as flooding, or an interruption in services such as a loss of power. One example of an alarm system is the burglar alarm commonly found in residential and commercial environments. Burglar alarms detect intrusions into unauthorized areas and notify either a local or remote security agency to react. To detect intrusions, these systems rely on a number of different types of sensors: motion detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors. **Motion detectors** detect movement within a confined space

and are either active or passive. Some motion sensors emit energy beams, usually in the form of infrared or laser light, ultrasonic sound or sound waves, or some form of electromagnetic radiation. If the energy from the beam projected into the area being monitored is disrupted, the alarm is activated. Other types of motion sensors are passive in that they constantly measure the energy (infrared or ultrasonic) from the monitored space and detect rapid changes in this energy. The passive measurement of these energies can be blocked or disguised and is therefore fallible. **Thermal detectors** measure rates of change in the ambient temperature in the room. They can, for example, detect when a person with a body temperature of 98.6 degrees Fahrenheit enters a room with a temperature of 65 degrees Fahrenheit, because the person's presence changes the room's ambient temperature. Thermal detectors are also used in fire detection (as is described in later sections). **Contact and weight sensors** work when two contacts are connected as, for example, when a foot steps on a pressure-sensitive pad under a rug, or a window is opened, triggering a pin-and-spring sensor. **Vibration sensors** also fall into this category, except that they detect movement of the sensor rather than movement in the environment.

Computer Rooms and Wiring Closets Computer rooms and wiring and communications closets require special attention to ensure the confidentiality, integrity, and availability of information. For an outline of the physical and environmental controls needed for computer rooms, read the Technical Details box entitled “Physical and Environmental Controls for Computer Rooms.”

Logical access controls are easily defeated if an attacker gains physical access to the computing equipment. Custodial staff members are often the least scrutinized employees (or nonemployees) who have access to an organization's offices. Yet custodians are given the greatest degree of unsupervised access. They are often handed the master keys to the entire building and then ignored, even though they collect paper from every office, dust many desks, and move large containers from every area. It is, therefore, not difficult for this type of worker to gather critical information and computer media or copy proprietary and classified information. All this is not to say that an organization's custodial staff should be under constant suspicion of espionage, but to note that the wide-reaching access that custodians have can be a vulnerability that attackers exploit to gain unauthorized information. Factual accounts exist of technically trained agents working as custodians in the offices of their competition. Thus, custodial staffs should be carefully managed not only by the organization's general management, but also by IT management.

Interior Walls and Doors The security of information assets can sometimes be compromised by the nature of the construction of the walls and doors of the facility. The walls in a facility are typically of two types: standard interior and firewall. Building codes require that each floor have a number of **firewalls**, or walls that limit the spread of damage should a fire break out in an office. While the network firewalls discussed in an earlier chapter isolate the logical subnetworks of the organization, physical firewalls isolate the physical spaces of the organization's offices. Between the firewalls, standard interior walls compartmentalize the individual offices. Unlike firewalls, these interior walls reach only part way to the next floor, which leaves a space above the ceiling but below the floor of the next level up. This space is called a **plenum**, and is usually one to three feet to allow for ventilation systems that can inexpensively collect return air from all the offices on the floor. For security, however, this design is not ideal, because it means that an individual can climb over the wall

from one office to the other. As a result, all high-security areas, such as computer rooms and wiring closets, must have firewall-grade walls surrounding them. This provides physical security not only from potential intruders, but also from fires.

The doors that allow access into high-security rooms should also be evaluated. Standard office-grade doors provide little or no security. For example, one of the authors of this textbook once locked himself out of his office by accidentally breaking the key off in the lock. When the locksmith arrived, he carried a curious contraption. Instead of disassembling the lock or deploying other locksmith secrets, he carried a long piece of heavy-duty wire, bent into the shape of a bow, with a string tied to each end. He slid one end of this bow through the one-inch gap under the door, stood it on one end and yanked the string. The wire bow slid over the door handle and the string looped over it. When the locksmith yanked the string, the door swung open. (Note: to see this device in action visit <http://gizmodo.com/5477600/hotel-locks-defeated-by-piece-of-wire-secured-by-towel>, or search on the term “hotel locks defeated by piece of wire.”) This information is not meant to teach you how to access interior offices but to warn you that no office is completely secure. How can you avoid this problem? In most interior offices, you can’t. Instead, IT security professionals must educate the organization’s employees about how to secure the information and systems within their offices.

To secure doors, install push or crash bars on computer rooms and closets. These bars are much more difficult to open from the outside than the standard door pull handles and thus provide much higher levels of security, but they also allow for safe egress in the event of an emergency.



Fire Security and Safety

The most important security concern is the safety of the people present in an organization’s physical space—workers, customers, clients, and others. The most serious threat to that safety is fire. Fires account for more property damage, personal injury, and death than any other threat to physical security. As a result, it is imperative that physical security plans examine and implement strong measures to detect and respond to fires and fire hazards.

Fire Detection and Response

Fire suppression systems are devices that are installed and maintained to detect and respond to a fire, potential fire, or combustion danger situation. These systems typically work by denying an environment one of the three requirements for a fire to burn: temperature (ignition source), fuel, and oxygen.

While the temperature of ignition, or **flame point**, depends upon the material, it can be as low as a few hundred degrees. Paper, the most common combustible in the office, has a flame point of 451 degrees Fahrenheit (a fact that is used to dramatic effect in Ray Bradbury’s novel *Fahrenheit 451*). Paper can reach that temperature when it is exposed to a carelessly dropped cigarette, malfunctioning electrical equipment, or other accidental or purposeful misadventures.

Water and water mist systems, which are described in detail in subsequent paragraphs, work both to reduce the temperature of the flame in order to extinguish it and to saturate some types of fuels (such as paper) to prevent ignition. Carbon dioxide systems (CO₂) rob fire of



Technical Details Physical and Environmental Controls for Computer Rooms

The following list of physical and environmental controls for computer rooms is intended to be representative, not comprehensive.

- Card keys for building and entrances to work area
- Twenty-four-hour guards at all entrances and exits
- Cipher lock on computer room door
- Raised floor in computer room
- Dedicated cooling system
- Humidifier in tape library
- Emergency lighting in computer room
- Four fire extinguishers rated for electrical fires
- One fire extinguisher with a combination of a class B and class C fire control rating (note that fire control ratings are discussed below)
- Smoke, water, and heat detectors
- Emergency power shutoff switch by exit door
- Surge suppressor
- Emergency replacement server
- Zoned dry-pipe sprinkler system
- Uninterruptible power supply for LAN servers
- Power strips and suppressors for peripherals
- Power strips and suppressors for computers
- Controlled access to file server room
- Plastic sheets for water protection
- Closed-circuit television monitors

Adapted from "Guide for Developing Security Plans for Information Technology Systems"⁴ by M. Swanson, NIST Special Publication 800-18, February 2006.

its oxygen. Soda acid systems deny fire its fuel, preventing the fire from spreading. Gas-based systems, such as Halon and its Environmental Protection Agency-approved replacements, disrupt the fire's chemical reaction but leave enough oxygen for people to survive for a short time. Before a fire can be suppressed, however, it must be detected.

Fire Detection Fire detection systems fall into two general categories: manual and automatic. **Manual fire detection systems** include human responses, such as calling the fire department, as well as manually activated alarms, such as sprinklers and gaseous systems. Organizations must use care when manually triggered alarms are tied directly to suppression systems, since false alarms are not uncommon. Organizations should also ensure that proper security remains in place until all employees and visitors have been cleared from the building and their evacuation has been verified. During the chaos of a fire evacuation, an attacker can easily slip into offices and obtain sensitive information. To help prevent such intrusions, fire safety programs often designate an individual from each office area to serve as a floor monitor.

There are three basic types of fire detection systems: thermal detection, smoke detection, and flame detection. **Thermal detection systems** contain a sophisticated heat sensor that operates in one of two ways. **Fixed temperature** sensors detect when the ambient temperature in an area reaches a predetermined level, usually between 135 degrees Fahrenheit and 165 degrees Fahrenheit, or 57 degrees Centigrade to 74 degrees Centigrade.⁵ **Rate-of-rise** sensors detect an unusually rapid increase in the area temperature within a relatively short period of time. In either case, if the criteria are met, the alarm and suppression systems are activated. Thermal detection systems are inexpensive and easy to maintain. Unfortunately, thermal detectors usually don't catch a problem until it is already in progress, as in a full-blown fire. As a result, thermal detection systems are not a sufficient means of fire protection in areas where human safety could be at risk. They are also not recommended for areas with high-value items or items that could be easily damaged by high temperatures.

Smoke detection systems are perhaps the most common means of detecting a potentially dangerous fire, and they are required by building codes in most residential dwellings and commercial buildings. Smoke detectors operate in one of three ways. **Photoelectric sensors** project and detect an infrared beam across an area. If the beam is interrupted (presumably by smoke), the alarm or suppression system is activated. **Ionization sensors** contain a small amount of a harmless radioactive material within a detection chamber. When certain by-products of combustion enter the chamber, they change the level of electrical conductivity within the chamber and activate the detector. Ionization sensor systems are much more sophisticated than photoelectric sensors and can detect fires much earlier, since invisible by-products can be detected long before enough visible material enters a photoelectric sensor to trigger a reaction. **Air-aspirating detectors** are sophisticated systems and are used in high-sensitivity areas. They work by taking in air, filtering it, and moving it through a chamber containing a laser beam. If the laser beam is diverted or refracted by smoke particles, the system is activated. These types of systems are typically much more expensive than systems that use photoelectric or ionization sensors; however, they are much better at early detection and are commonly used in areas where extremely valuable materials are stored.


The third major category of fire detection systems is the **flame detector**. The flame detector is a sensor that detects the infrared or ultraviolet light produced by an open flame. These systems compare a scanned area's light signature to a database of known flame light signatures to determine whether or not to activate the alarm and suppression systems. While highly sensitive, flame detection systems are expensive and must be installed where they can scan all areas of the protected space. They are not typically used in areas with human lives at stake; however, they are quite suitable for chemical storage areas where normal chemical emissions might activate smoke detectors.



Fire Suppression Fire suppression systems can consist of portable, manual, or automatic apparatus. Portable extinguishers are used in a variety of situations where direct application of suppression is preferred, or fixed apparatus is impractical. Portable extinguishers are much more efficient for smaller fires, because triggering an entire building's sprinkler systems can do a lot of damage. Portable extinguishers are rated by the type of fire they can combat, as follows:

- **Class A fires:** Those fires that involve ordinary combustible fuels such as wood, paper, textiles, rubber, cloth, and trash. **Class A fires** are extinguished by agents that interrupt the ability of the fuel to be ignited. Water and multipurpose dry chemical fire extinguishers are ideal for these types of fires.
- **Class B fires:** Those fires fueled by combustible liquids or gases, such as solvents, gasoline, paint, lacquer, and oil. **Class B fires** are extinguished by agents that remove oxygen from the fire. Carbon dioxide, multipurpose dry chemical, and Halon fire extinguishers are ideal for these types of fires.
- **Class C fires:** Those fires with energized electrical equipment or appliances. **Class C fires** are extinguished with non-conducting agents only. Carbon dioxide, multipurpose dry chemical, and Halon fire extinguishers are ideal for these types of fires. Never use a water fire extinguisher on a Class C fire.
- **Class D fires:** Those fires fueled by combustible metals, such as magnesium, lithium, and sodium. **Class D fires** require special extinguishing agents and techniques.

The Technical Details box on Halon and the EPA describes the ban on new installations of Halon-based systems and lists the approved replacements.



Technical Details Halon Q & A

Halon Substitutes Under SNAP as of 21 August 2003⁶

When was the production of Halons banned?

Under the Clean Air Act (CAA), the United States banned the production and import of virgin Halons 1211, 1301, and 2402 beginning January 1, 1994, in compliance with the Montreal Protocol on Substances that Deplete the Ozone Layer. Recycled Halon and inventories produced before January 1, 1994 are now the only sources of supply. EPA's final rule published March 5, 1998 (63 FR 11084) bans the formulation of any blend of two or more of these Halons with one exception. An exemption is provided for Halon blends formulated using recycled Halon solely for the purpose of aviation fire protection, provided that blends produced under this exemption are recycled to meet the relevant purity standards for each individual Halon. A fact sheet summarizing this rule is also available from the Stratospheric Ozone Protection Hotline.

Must I now dismantle my Halon fire protection system?

No. It is legal to continue to use your existing Halon system. It is even legal to purchase recycled Halon and Halon produced before the phase-out to recharge your system.

However, because Halons deplete the ozone layer, users are encouraged to consider replacing their system and making their Halon stock available for users with more critical needs.

Are there any federal laws on emissions of Halons?

EPA's final rule published March 5, 1998 (63 FR 11084) prohibits the intentional release of Halon 1211, Halon 1301, and Halon 2402 during the testing, repairing, maintaining, servicing, or disposal of Halon-containing equipment or during the use of such equipment for technician training. The rule also requires appropriate training of technicians regarding emissions reduction and proper disposal of Halon and Halon-containing equipment. The rule became effective April 6, 1998.

What are the acceptable substitutes for Halon?

There are a number of acceptable substitutes for Halon 1211 and 1301 (the two most common types of Halon-based systems).

The various options are summarized in Table 9-1.

Acceptable Substitutes for Halon 1211 Streaming Agents Under the Significant New Alternatives Policy (SNAP) Program as of 5 July 2007⁷		
Substitute	Trade Name	Comments
HCFC-123	FE-232	Nonresidential uses only
HCFC-124	FE-241	Nonresidential uses only
[HCFC Blend] B	Halotron 1	Nonresidential uses only
[HCFC Blend] C	NAF P-III	Nonresidential uses only
[HCFC Blend] D	Blitz III	Nonresidential uses only
Gelled Halocarbon / Dry chemical suspension	Envirogel	Allowable in the residential use market
[Surfactant Blend] A	Cold Fire, Flameout	
Water mist systems using potable or natural sea water		
Carbon dioxide		
Dry chemical		
Foam		

Table 9-1 Acceptable Substitutes

Acceptable Substitutes for Halon 1211 Streaming Agents Under the Significant New Alternatives Policy (SNAP) Program as of 5 July 2007		
Substitute	Trade Name	Comments
Powdered Aerosol C	PyroGen, Dynameco	For use in unoccupied areas only
Powdered Aerosol A	SFE	For use in unoccupied areas only
Carbon dioxide system		Design must adhere to OSHA 1910.162(b)(5) and NFPA Standard 12
Water		Water mist systems using potable or natural sea water
Foam A	Phirex+	This agent is not a clean agent, but is a low-density, short duration foam
HCFC-22		Use of this agent and all following agents must be in accordance with safety guidelines in NFPA 2001 standard for clean agent fire extinguishing systems
HCFC-124 HCFC Blend A (NAF S-III)	FE-241	
HFC-23 (FE-13)		
HFC-125 (FE 25)		
HFC-227ea (FM-200, FE-227)		
HFC-134a		
IG-100 (NM 100)		
IG-01 (Argotec; formally Inert Gas Blend C)		
IG-55 (Argonite; formally Inert Gas Blend B)		
IG-541 (Inergen)		
C6-perfluoroketone [1,1,1,2,2,4,5,5,5-nonafluoro-4-(trifluoromethyl)-3-pentanone] (Novec 1230)		
Gelled Halocarbon/Dry Chemical Suspension (Envirogel) with ammonium polyphosphate additive		
HFC-125 with 0.1% d-limonene (NAF S-125) HFC-227ea with 0.1% d-limonene (NAF S 227)		

Table 9-1 Acceptable Substitutes (continued)*From The Environmental Protection Agency, Online, 7 July 2007.*

Manual and automatic fire response systems include those designed to apply suppressive agents. These are usually either sprinkler or gaseous systems. All **sprinkler systems** are designed to apply liquid, usually water, to all areas in which a fire has been detected, but an organization can choose from one of three implementations: wet-pipe, dry-pipe, or pre-action systems. A **wet-pipe** system has pressurized water in all pipes and has some form of valve in each protected area. When the system is activated, the valves open, sprinkling the area. This is best for areas where the fire represents a serious risk to people, but where damage to property is not a major concern. The most obvious drawback to this type of system is water damage to office equipment and materials. A wet-pipe system is not usually appropriate in computer rooms, wiring closets, or anywhere electrical equipment is used or stored. There is also the risk of accidental or unauthorized activation. Figure 9-3 shows a wet-pipe water sprinkler system that is activated when the ambient temperature reaches 140 degrees Fahrenheit to 150 degrees Fahrenheit, bringing the special liquid in the glass tube to a boil, which causes the tube to shatter and open the valve. Once the valve is open, water flows through the diffuser, which disperses the water over the area.

A **dry-pipe system** is designed to work in areas where electrical equipment is used. Instead of water, the system contains pressurized air. The air holds valves closed, keeping the water away from the target areas. When a fire is detected, the sprinkler heads are activated, the pressurized air escapes, and water fills the pipes and exits through the sprinkler heads. This reduces the risk of accidental leakage from the system. Some sprinkler system, called **deluge systems**, keep open all of the individual sprinkler heads, and as soon as the system is activated, water is immediately applied to all areas. This is not, however, the optimal solution



Figure 9-3 Water Sprinkler System

Source: *Course Technology/Cengage Learning*

for computing environments, since there are other more sophisticated systems that can suppress the fire without damage to computer equipment.

A variation of the dry-pipe system is the **pre-action system**. This approach has a two-phase response to a fire. Under normal conditions, the system has nothing in the delivery pipes. When a fire is detected, the first phase is initiated, and valves allow water to enter the system. At that point, the system resembles a wet-pipe system. The pre-action system does not deliver water into the protected space until the individual sprinkler heads are triggered, at which time water flows only into the area of the activated sprinkler head.

Water mist sprinklers are the newest form of sprinkler systems and rely on ultra-fine mists instead of traditional shower-type systems. The water mist systems work like traditional water system by reducing the ambient temperature around the flame, therefore minimizing its ability to sustain the necessary temperature needed to maintain combustion. Unlike traditional water sprinkler systems, however, these systems produce a fog-like mist that, because the droplets are much less susceptible to gravity, stays buoyant (airborne) much longer. As a result, a much smaller quantity of water is required; also the fire is extinguished more quickly, which causes less collateral damage. Relative to gaseous systems (which are discussed shortly), water-based systems are low cost, nontoxic, and can often be created by using an existing sprinkler system that may have been present in earlier construction.

Gaseous Emission Systems Gaseous (or chemical gas) emission systems can be used in the suppression of fires. They are often used to protect chemical and electrical processing areas, as well as facilities that house computing systems. A typical configuration of such systems is shown in Figure 9-4.

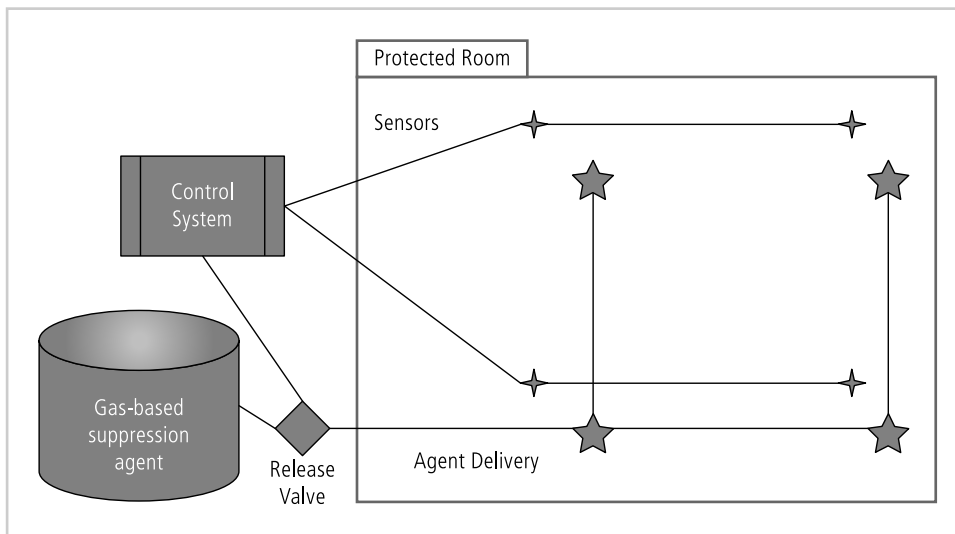


Figure 9-4 Gaseous Fire Suppression System

Source: Course Technology/Cengage Learning

Gaseous fire suppression systems are either self-pressurizing or must be pressurized with an additional agent. Until recently there were only two major types of gaseous systems: carbon dioxide and Halon. Carbon dioxide extinguishes a fire by removing its supply of oxygen. Unfortunately, any living organisms that also rely on oxygen are similarly extinguished. As a result, carbon dioxide systems are not commonly used in residential or office environments where people or animals are likely to be present. The alternative is Halon. Halon is one of a few chemicals designated as a **clean agent**, which means that it does not leave any residue after use, nor does it interfere with the operation of electrical or electronic equipment. As a result, Halon gas-based systems are the preferred solution for computer rooms and communications closets. Unlike carbon dioxide, Halon does not rob the fire of its oxygen but instead relies on a chemical reaction with the flame to extinguish it. As a result, Halon is much safer than carbon dioxide when people or animals are present. Although Halon can cause suffocation like a carbon dioxide system, the dosage levels required are much higher, and therefore Halon-based systems provide additional time for people to exit areas. Because the EPA has classified Halon as an ozone-depleting substance, new installations of the controlled types of Halon are prohibited in commercial and residential locations. There are a number of alternatives, as presented in Table 9-1 in the Technical Details box called Halon Q & A although, as is often the case, the alternatives are reported to be less effective than Halon.

A physical security plan requires that every building have clearly marked fire exits and maps posted throughout the facility. It is important to have drills to rehearse fire alarm responses and designate individuals to be in charge of escorting everyone from the location and ensuring that no one is left behind. It is also important to have fire suppression systems that are both manual and automatic, and that are inspected and tested regularly.



Failure of Supporting Utilities and Structural Collapse

Supporting utilities, such as heating, ventilation and air conditioning, power, water, and other utilities, have a significant impact on the safe operation of a facility. Extreme temperatures and humidity levels, electrical fluctuations and the interruption of water, sewage, and garbage services can create conditions that inject vulnerabilities in systems designed to protect information. Thus, each of these utilities must be properly managed in order to prevent damage to information and information systems.

Heating, Ventilation, and Air Conditioning

Although traditionally a facilities management responsibility, the operation of the heating, ventilation, and air-conditioning (HVAC) system can have dramatic impact on information and information systems operations and protection. Specifically, the temperature, filtration, humidity, and static electricity controls must be monitored and adjusted to reduce risks to information systems.

Temperature and Filtration Computer systems are electronic, and as such are subject to damage from extreme temperature and particulate contamination. Temperatures as low as 100 degrees Fahrenheit can damage computer media, and at 175 degrees Fahrenheit, computer hardware can be damaged or destroyed. When the temperature approaches

32 degrees Fahrenheit, media are susceptible to cracking and computer components can actually freeze together. Rapid changes in temperature, from hot to cold or from cold to hot, can produce condensation, which can create short circuits or otherwise damage systems and components. The optimal temperature for a computing environment (and for people) is between 70 and 74 degrees Fahrenheit. Properly installed and maintained systems keep the environment within the manufacturer-recommended temperature range. In the past it was thought necessary to fully filter all particles from the air flow from the HVAC system. Modern computing equipment is designed to work better in typical office environments, and thus the need to provide extensive filtration for air-conditioning is now limited to particularly sensitive environments such as chip fabrication and component assembly areas. In other words, filtration is no longer as significant a factor as it once was for most commercial data processing facilities.

Humidity and Static Electricity Humidity is the amount of moisture in the air. High humidity levels create condensation problems, and low humidity levels can increase the amount of static electricity in the environment. With condensation comes the short-circuiting of electrical equipment and the potential for mold and rot in paper-based information storage. **Static electricity** is caused by a process called **triboelectrification**, which occurs when two materials make contact and exchange electrons, and results in one object becoming more positively charged and the other more negatively charged. When a third object with an opposite charge or ground is encountered, electrons flow again, and a spark is produced. One of the leading causes of damage to sensitive circuitry is **electrostatic discharge (ESD)**. Integrated circuits in a computer are designed to use between two and five volts of electricity; any voltage level above this range introduces a risk of microchip damage. Static electricity is not even noticeable to humans until levels approach 1,500 volts, and the spark can't be seen until the level approaches 4,000 volts. Moreover, a person can generate up to 12,000 volts of static current by merely walking across a carpet. Table 9-2 shows some static charge voltages and the damage they can cause to systems.

In general, ESD damage to chips produces two types of failures. Immediate failures, also known as catastrophic failures, occur right away, are usually totally destructive, and require chip replacement. Latent failures or delayed failures can occur weeks or even months after the damage occurs. The damage may not be noticeable, but the chip may suffer intermittent problems. (It has been observed, however, that with the overall poor quality of some of the current popular operating systems, this type of damage may be hard to notice.) As a result, it is imperative to maintain the optimal level of humidity, which is between 40 percent and

Volts	Results
40	High probability of damage to sensitive circuits and transistors
1,000	Scrambles monitor display
1,500	Can cause disk drive data loss
2,000	High probability of system shutdown
4,000	May jam printers
17,000	Causes certain and permanent damage to almost all microcircuitry

Table 9-2 Static Charge Damage in Computers⁸

60 percent, in the computing environment. Humidity levels below this range create static, and levels above create condensation. Humidification or dehumidification systems can regulate humidity levels.

Ventilation Shafts While the ductwork in residential buildings is quite small, in large commercial buildings, it may be large enough for a person to climb through. This is one of Hollywood's favorite methods for villains or heroes to enter buildings, but these ventilation shafts aren't quite as negotiable as the movies would have you believe. In fact, with moderate security precautions, these shafts can be completely eliminated as a security vulnerability. In most new buildings, the ducts to the individual rooms are no larger than 12 inches in diameter and are flexible, insulated tubes. The size and nature of the ducts precludes most people from using them, but access may be possible via the plenum. If the ducts are much larger, the security team can install wire mesh grids at various points to compartmentalize the runs.

Power Management and Conditioning

Electrical power is another aspect of the organization's physical environment that is usually considered within the realm of physical security. It is critical that power systems used by information-processing equipment be properly installed and correctly grounded. Interference with the normal pattern of the electrical current is referred to as **noise**. Because computers sometimes use the normal 60 Hertz cycle of the electricity in alternating current to synchronize their clocks, noise that interferes with this cycle can result in inaccurate time clocks or, even worse, unreliable internal clocks inside the CPU.

Grounding and Amperage Grounding ensures that the returning flow of current is properly discharged to the ground. If the grounding elements of the electrical system are not properly installed, anyone touching a computer or other electrical device could become a ground source, which would cause damage to equipment and injury or death to the person. Computing and other electrical equipment in areas where water can accumulate must be uniquely grounded, using **ground fault circuit interruption** (GFCI) equipment. GFCI is capable of quickly identifying and interrupting a ground fault—that is, a situation in which a person has come into contact with water and becomes a better ground than the electrical circuit's current source.

Power should also be provided in sufficient amperage to support needed operations. Nothing is more frustrating than plugging in a series of computers, only to have the circuit breaker trip. Consult a qualified electrician when designing or remodeling computer rooms to make sure sufficiently high amperage circuits are available to provide the needed power. Overloading a circuit not only trips circuit breakers, but can also create a load on an electrical cable that is in excess of what the cable is rated to handle, and thus increase the risk of its overheating and starting a fire.

Uninterruptible Power Supply (UPS) The primary power source for an organization's computing equipment is most often the electric utility that serves the area where the organization's buildings are located. This source of power can experience interruptions. Therefore, organizations should identify the computing systems that are critical to their operations (in other words, the systems that must continue to operate during interruptions) and make sure those systems are connected to a device that assures the delivery of electric power without interruption—that is, an uninterruptible power supply (UPS).



The capacity of UPS devices is measured using the volt-ampere (or VA) power output rating. UPS devices typically run up to 1,000 VA and can be engineered to exceed 10,000 VA. A typical PC might use 200 VA, and a server in a computer room may need 2,000 to 5,000 VA, depending on how much running time is needed. Figure 9-5 shows a number of types of UPS. This section describes the following basic configurations: the standby, line-interactive, standby on-line hybrid, standby-ferro, double conversion online (also known as true online), and delta conversion online.

A **standby** or **offline UPS** is an offline battery backup that detects the interruption of power to the equipment and activates a transfer switch that provides power from batteries, through a DC to AC converter, until the power is restored or the computer is shut down. Because this type of UPS is not truly uninterruptible, it is often referred to as a standby power supply (SPS). The advantage of an SPS is that it is the most cost-effective type of UPS. However, the significant drawbacks, such as the limited run time and the amount of time it takes to switch from standby to active, may outweigh the cost savings. Switching time may also become an issue because very sensitive computing equipment may not be able to handle the transfer delay, and may reset and suffer data loss or damage. Also, SPS systems do not provide power conditioning, a feature of more sophisticated UPSs (discussed below). As a result, an SPS is seldom used in critical computing applications and is best suited for home and light office use.

A **ferroresonant standby UPS** improves upon the standby UPS design. It is still an offline UPS, with the electrical service providing the primary source of power and the UPS serving as a battery backup. The primary difference is that a ferroresonant transformer replaces the UPS transfer switch. The transformer provides line filtering to the primary power source, reducing the effect of some power problems and reducing noise that may be present in the power as it is delivered. This transformer also stores energy in its coils, thereby providing a buffer to fill in the gap between the interruption of service and the activation of an alternate source of power (usually a battery backup). This greatly reduces the probability of system reset and data loss. Ferroresonant standby UPS systems are better suited to settings that require a large capacity of conditioned and reliable power, since they are available for uses up to 14,000 VA. With the improvement in other UPS designs, however, many manufacturers have abandoned this design in favor of other configurations.

The **line-interactive UPS** has a substantially different design than the previously mentioned UPS models. In line-interactive UPSs, the internal components of the standby models are replaced with a pair of inverters and converters. The primary power source, as in both the SPS and the ferroresonant UPS, remains the power utility company, with a battery serving as backup. However, the inverters and converters both charge the battery and provide power when needed. When utility power is interrupted, the converter begins supplying power to the systems. Because this device is always connected to the output as opposed to relying on a switch, this model has a much faster response time and also incorporates power conditioning and line filtering.

In a **true online UPS**, the primary power source is the battery, and the power feed from the utility is constantly recharging this battery. This model allows constant use of the system, while completely eliminating power fluctuation. True online UPS can deliver a constant, smooth, conditioned power stream to the computing systems. If the utility-provided power fails, the computer systems are unaffected as long as the batteries hold out. The online UPS is considered the top-of-the-line option and is the most expensive. The only major

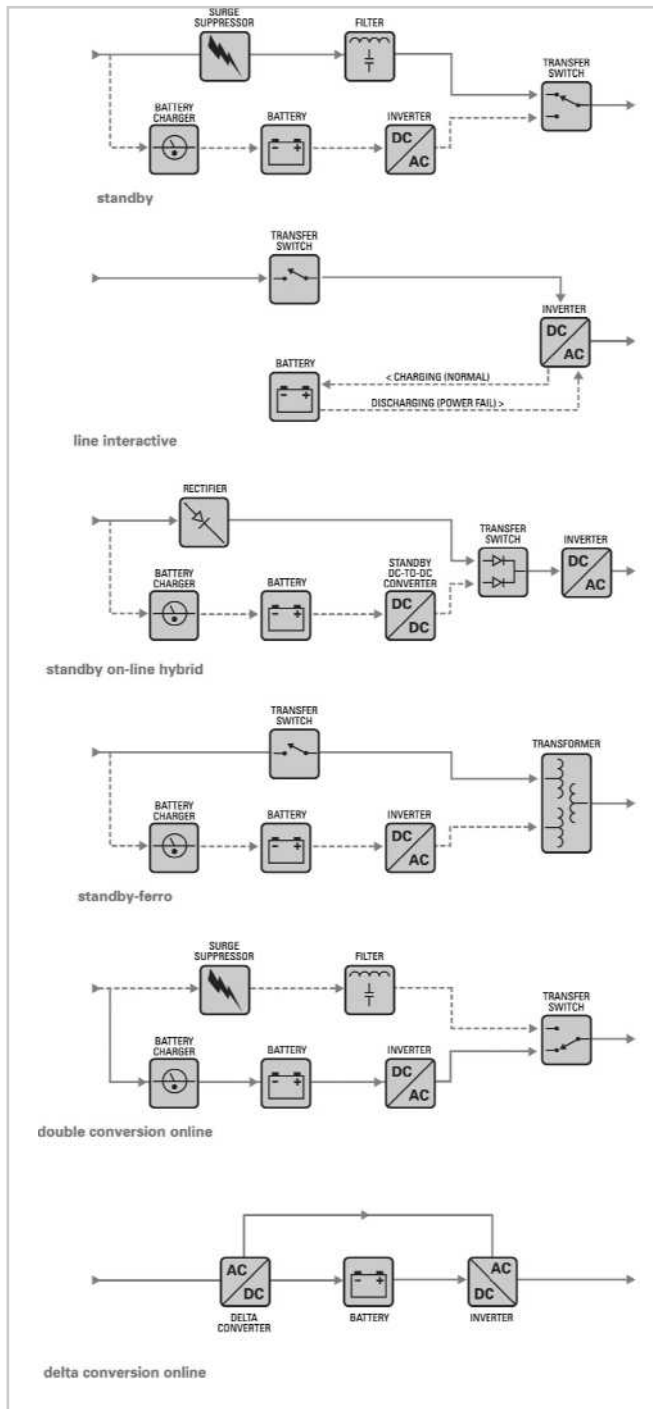


Figure 9-5 Types of Uninterruptible Power Supplies⁹

Source: Courtesy of American Power Conversion Corporation

drawback, other than cost, is that the process of constantly converting from the AC feed from the utility to the DC used by the battery storage and then converting back to AC for use by the systems generates a lot of heat. An improved model resolves this issue by incorporating a device known as a delta-conversion unit, which allows some of the incoming power to be fed directly to the destination computers, thus reducing the amount of energy wasted and heat generated. Should the power fail, the delta unit shuts off, and the batteries automatically compensate for the increased power draw.

Selecting the best UPS can be a lesson in electrical engineering, because you must calculate the load that the protected systems require from the UPS. This can be quite complex and proves challenging in practice. Fortunately, many UPS vendors provide sample scenarios that can help you select the optimal device. Because a high-quality UPS may cost several thousand dollars, it is advisable to select the smallest UPS necessary to provide the desired effect. To calculate manually the rating needed in a UPS, you should begin by reviewing the computer systems and all connected support equipment to be protected. For example, the back panel of a monitor may indicate that the monitor is rated at 110 volts and 2 amps. Since volts times amps yields the power needs of a device, to calculate the power you need to run this device, you multiply 110 by 2; the production of this equation is the rating of the monitor, 220 VA. Now suppose the computer draws 3 amps at 110 volts, and therefore has a rating of 330 VA. Together the total is 550 VA. Once you have this information, you can select a UPS capable of supporting this power level. Generally, UPS systems provide information on how long they would run at specific VA levels. Some smaller-scale UPSs can run for approximately six minutes at 600 VA at full voltage. You should look for a UPS that provides enough time for the computing equipment to ride out minor power fluctuations, and for the user to shut down the computer safely if necessary.

Emergency Shutoff One important aspect of power management in any environment is the ability to stop power immediately should the current represent a risk to human or machine safety. Most computer rooms and wiring closets are equipped with an emergency power shutoff, which is usually a large red button that is prominently placed to facilitate access, and has a cover to prevent unintentional use. These devices are the last line of defense against personal injury and machine damage in the event of flooding or sprinkler activation. The last person out of the computer room hits the switch to stop the flow of electricity to the room, preventing the water that might be used to extinguish the fire from short-circuiting the computers. While it is never advisable to allow water to come into contact with a computer, there is a much higher probability of recovering the systems if they were not powered up when they got wet. At a minimum, hard drives and other sealed devices may be recoverable. Some disaster recovery companies specialize in water damage recovery.

Water Problems

Another critical utility infrastructure element is water service. On the one hand, lack of water poses problems to systems, including fire suppression and air-conditioning systems. On the other hand, a surplus of water, or water pressure, poses a real threat. Flooding, leaks, and the presence of water in areas where it should not be is catastrophic to paper and electronic storage of information. Water damage can result in complete failure of computer systems and the structures that house them. It is therefore important to integrate water detection systems into the alarm systems that regulate overall facilities operations.

Structural Collapse

Unavoidable environmental factors or forces of nature can cause failures in the structures that house the organization. Structures are designed and constructed with specific load limits, and overloading these design limits inevitably results in structural failure. Personal injury and potential for loss of life are also likely. Scheduling periodic inspections by qualified civil engineers will enable managers to identify potentially dangerous structural conditions before the structure fails.

Maintenance of Facility Systems

Just as with any phase of the security process, the implementation of the physical security phase must be constantly documented, evaluated, and tested; once the physical security of a facility is established, it must be diligently maintained. Ongoing maintenance of systems is required as part of the systems' operations. Documentation of the facility's configuration, operation, and function should be integrated into disaster recovery plans and standard operating procedures. Testing provides information necessary to improve the physical security in the facility and identifies weak points.

Interception of Data

There are three methods of data interception: direct observation, interception of data transmission, and electromagnetic interception. The first method, *direct observation*, requires that an individual be close enough to the information to breach confidentiality. The physical security mechanisms described in the previous sections limit the possibility of an individual accessing unauthorized areas and directly observing information. There is, however, a risk when the information is removed from a protected facility. If an employee is browsing documents over lunch in a restaurant or takes work home, the risk of direct observation rises substantially. A competitor can more easily intercept vital information at a typical employee's home than at a secure office. Incidences of interception, such as shoulder surfing, can be avoided if employees are prohibited from removing sensitive information from the office or required to implement strong security at their homes.

The second method, *interception of data transmissions*, has become easier in the age of the Internet. If attackers can access the media transmitting the data, they needn't be anywhere near the source of the information. In some cases, the attacker can use sniffer software, which was described in previous chapters, to collect data. Other means of interception, such as tapping into a LAN, require some proximity to the organization's computers or networks. It is important for network administrators to conduct periodic physical inspections of all data ports to ensure that no unauthorized taps have occurred. If direct wiretaps are a concern, the organization should consider using fiber-optic cable, as the difficulty of splicing into this type of cable makes it much more resistant to tapping. If wireless LANs are used, the organization should be concerned about eavesdropping, since an attacker can snoop from a location that can be—depending on the strength of the wireless access points (WAPs)—hundreds of feet outside the organization's building. Since wireless LANs are uniquely susceptible to eavesdropping, and current generation wireless sniffers are very potent tools, all wireless communications should be secured via encryption. Incidentally, it may interest you to know that the U.S. federal laws that deal with wiretapping do not cover wireless communications, except



for commercial cellular phone calls; courts have ruled that users have no expectation of privacy with radio-based communications media.

The third method of data interception, *electromagnetic interception*, sounds like it could be from a *Star Trek* episode. For decades, scientists have known that electricity moving through cables emits electromagnetic signals (EM). It is possible to eavesdrop on these signals and therefore determine the data carried on the cables without actually tapping into them. In 1985, scientists proved that computer monitors also emitted radio waves, and that the image on the screens could be reconstructed from these signals.¹⁰ More recently, scientists have determined that certain devices with LED displays actually emit information encoded in the light that pulses in these LEDs.¹¹

Whether devices that emit **electromagnetic radiation** (EMR) can actually be monitored such that the data being processed or displayed can be reconstructed has been a subject of debate (and rumor) for many years. James Atkinson, an electronics engineer certified by the National Security Agency (NSA), says that there is no such thing as practical monitoring of electronic emanations and claims that stories about such monitoring are just urban legends. He goes on to say that most modern computers are shielded to prevent interference with other household and office equipment—not to prevent eavesdropping. Atkinson does concede that receiving emanations from a computer monitor is theoretically possible, but notes that it would be an extremely difficult, expensive, and impractical undertaking.¹²

Legend or not, a good deal of money is being spent by the government and military to protect computers from electronic remote eavesdropping. In fact, the U.S. government has developed a program, named **TEMPEST**, to reduce the risk of EMR monitoring. (In keeping with the speculative fancy surrounding this topic, some believe that the acronym TEMPEST was originally a code word created by the U.S. government in the 1960s, but was later defined as Transient Electromagnetic Pulse Emanation Surveillance Technology or Telecommunications Electronics Material Protected from Emanating Spurious Transmissions.) In general, TEMPEST involves the following procedures: ensuring that computers are placed as far as possible from outside perimeters, installing special shielding inside the CPU case, and implementing a host of other restrictions, including maintaining distances from plumbing and other infrastructure components that carry radio waves. Additional information about this subject and the controls that have been developed can be found at www.fas.org/irp/program/security/tempest.htm or www.cnss.gov/Assets/pdf/nstissam_tempest_1-00.pdf. Regardless of whether the threat from eavesdropping on electromagnetic emanations is real, many procedures that protect against emanations also protect against threats to physical security.

Mobile and Portable Systems

Mobile computing requires even more security than the average in-house system. Most mobile computing systems—laptops, handhelds, and PDAs—have valuable corporate information stored within them, and some are configured to facilitate user access into the organization's secure computing facilities. Forms of access include VPN connections, dial-up configurations, and databases of passwords. In addition, many users keep the locations of files and clues about the storage of information in their portable computers. Many users like the convenience of allowing the underlying operating systems to remember their usernames and passwords because it provides easier access and because they frequently have multiple accounts, with

different usernames and passwords, to manage. While it is tempting to allow operating systems to enable easier access to frequently used accounts, the downside of setting up these arrangements on a portable system is obvious: loss of the system means loss of the access control mechanisms.

A relatively new technology to help locate lost or stolen laptops can provide additional security. For example, Absolute Software's CompuTrace Laptop Security is computer software that is installed on a laptop, as illustrated in Figure 9-6. Periodically, when the computer is on the Internet, the software reports itself and the electronic serial number of the computer on which it is installed to a central monitoring center. If the laptop is reported stolen, this software can trace the computer to its current location for possible recovery. The software is undetectable on the system, even if the thief knows the software is installed. Moreover, CompuTrace remains installed even if the laptop's hard drive is formatted and the operating system is reinstalled.

Also available for laptops are burglar alarms made up of a PC card or other device that contains a motion detector. If the device is armed, and the laptop is moved more than expected, the alarm triggers a very loud buzzer or horn. The security system may also disable the computer or use an encryption option to render the information stored in the system unusable.

For maximum security, laptops should be secured at all times. If you are traveling with a laptop, you should have it in your possession at all times. Special care should be exercised when flying, as laptop thefts are common in airports. The following list comes from the Metropolitan Police of the District of Columbia and outlines steps you can take to prevent your laptop from being stolen or carelessly damaged:

- Don't leave a laptop in an unlocked vehicle, even if the vehicle is in your driveway or garage, and never leave it in plain sight, even if the vehicle is locked—that's just inviting trouble. If you must leave your laptop in a vehicle, the best place is in a locked trunk. If you don't have a trunk, cover it up and lock the doors.
- Parking garages are likely areas for thefts from vehicles, as they provide numerous choices and cover for thieves. Again, never leave your laptop in plain sight; cover it or put it in the trunk.
- Do be aware of the damage extreme temperatures can cause to computers.

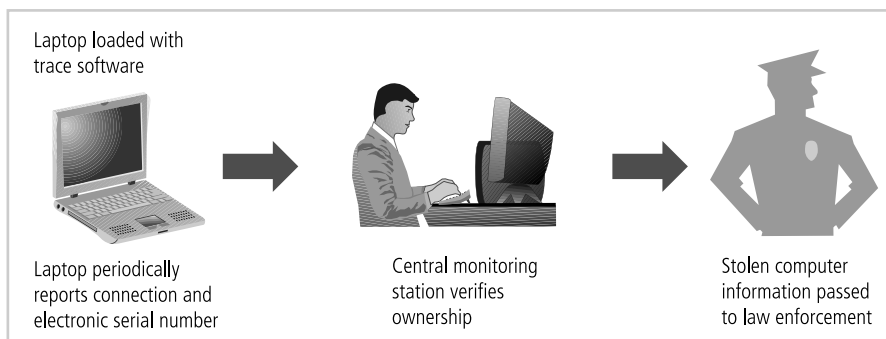


Figure 9-6 Laptop Theft Deterrence

Source: *Course Technology/Cengage Learning*

- Carry your laptop in a nondescript carrying case, briefcase, or bag when moving about. Placing it in a case designed for computers is an immediate alert to thieves that you have a laptop.
- Going to lunch or taking a break? Don't leave a meeting or conference room without your laptop. Take it with you, or you run the risk that it won't be there when you return.
- Lock the laptop in your office during off-hours. Don't have your own office? Use a cable lock that wraps around a desk or chair leg, or put the laptop in a locked closet or cabinet.
- Don't let unaccompanied strangers wander around in your workplace. Offer assistance and deliver the visitors to their destinations.
- Apply distinctive paint markings to make your laptop unique and easily identifiable. Liquid white-out is a good substance to apply.
- Consider purchasing one of the new theft alarm systems specially made for laptops.
- Be aware that if your computer is stolen, automatic logins can make it easy for a thief to send inappropriate messages with your account.
- Back up your information on disks today, and store the disks at home or the office.¹³

Remote Computing Security

Remote site computing, which is becoming increasingly popular, involves a wide variety of computing sites that are distant from the base organizational facility and includes all forms of telecommuting. **Telecommuting** is off site computing that uses Internet connections, dial-up connections, connections over leased point-to-point links between offices, and other connection mechanisms.

Telecommuting from users' homes deserves special attention. One of the appeals of telecommuting for both the employee and employer is that by avoiding physical commuting, telecommuting employees have more time to focus on the work they do. But as more people become telecommuters, the risk to information traveling via the often unsecured connections that telecommuters use is substantial. The problem is that not enough organizations provide secure connections to their office networks, and even fewer provide secure systems, should the employee's home computer be compromised. To secure the entire network, the organization must dedicate security resources to protecting these home connections. Although the installation of a VPN may go a long way toward protecting the data in transmission, telecommuters frequently store office data on their home systems, in home filing cabinets, and on off-site media. To ensure a secure process, the computers that telecommuters use must be made *more* secure than the organization's systems, as they are outside the security perimeter. An attacker breaking into someone's home would probably find a much lower level of security than at an office. Most office systems require users to log in, but the telecommuter's home computer is probably the employee's personal machine, and thus is likely to have a much less secure operating system and may not use a password. Telecommuters must use a securable operating system that requires password authentication, such as Windows XP/Vista/7 or Server 2003/2008. They must store all loose data in locking filing cabinets and loose media in locking fire safes. They must handle data at home more carefully than they would at the office, since the general level of security for the average home is lower than that of a commercial building.

The same applies to workers using mobile computers on the road. Employees using notebooks in hotel rooms should presume that their unencrypted transmissions are being monitored, and that any unsecured notebook computer can be stolen. The off-site worker using leased facilities does not know who else is physically attached to the network and therefore who might be listening to his or her data conversations. VPNs are a must in all off-site-to-on-site communications, and the use of associated advanced authentication systems is strongly recommended.

Although it is possible to secure remote sites, organizations cannot assume that employees will invest their own funds for security. Many organizations barely tolerate telecommuting for a number of reasons, including that telecommuting employees generally require two sets of computing equipment, one for the office and one for the home. This extra expense is difficult to justify, especially when the employee is the only one gaining the benefit from telecommuting. In those rare cases in which allowing an employee or consultant to telecommute is the only way to gain extremely valuable skills, the organization is usually willing to do what is necessary to secure its systems. Only when additional research into telecommuting clearly displays a bottom-line advantage do organizations begin to invest sufficient resources into securing the equipment of their telecommuters. However, there are some organizations that support telecommuting, and these organizations typically fall into one of three groups. The first is the mature and therefore fiscally sound organization with a sufficient budget to support telecommuting and thus enhance its standing with employees and its organizational image. In recent years, the option to telecommute has become a factor in the organizational rankings undertaken by various magazines. Some organizations seek to improve employee work conditions and also improve their position in the best-places-to-work ranking by adding telecommuting as an option for employees. The second group is the new high-technology company, with a large number of geographically diverse employees who telecommute almost exclusively. These companies use technology extensively and are determined to make the adoption of technology and its use the cornerstone of their organizations. The third group overlaps with the second and is called a virtual organization. A **virtual organization** is a group of individuals brought together for a specific task, usually from different organizations, divisions, or departments. These individuals form a virtual company, either in leased facilities or through 100-percent telecommuting arrangements. When the job is done, the organization is either redirected or dissolved. These organizations rely almost exclusively on remote computing and telecommuting, but they are extremely rare and therefore not well documented or studied.



Special Considerations for Physical Security

There are a number of special considerations to take into account when developing a physical security program. The first of these is the question of whether to handle physical security in-house or to outsource it. As with any aspect of information security, the make-or-buy decision should not be made lightly. There are a number of qualified and professional agencies that provide physical security consulting and services. The benefits of outsourcing physical security include gaining the experience and knowledge of these agencies, many of which have been in the field for decades. Outsourcing unfamiliar operations always frees an organization to focus on its primary objectives, rather than support operations. The downside includes the expense, the loss of control over the individual components of the physical security solution, and the need to trust another company to perform an essential business function. An organization

must not only trust the processes used by the contracted company, but also its ability to hire and retain trustworthy employees who respect the security of the contracting company even though they have no allegiance to it. This level of trust is often the most difficult aspect of the decision to outsource, because the reality of outsourcing physical security is that none-employees will be providing a safeguard that the organization administers only marginally.

Another physical security consideration is social engineering. As you learned in previous chapters, social engineering involves using people skills to obtain confidential information from employees. While most social engineers prefer to use the telephone or computer to solicit information, some attempt to access the information more directly. As in the previously mentioned cases in which technically proficient agents are placed into janitorial positions at a competitor's office, there are a number of ways an outsider can gain access to an organization's resources. Most organizations do not, for example, have very thorough procedures for authenticating and controlling nonemployees who access their facility. When there is no procedure in place, no one gives the wandering repairman, service worker, or city official a second look. It is not difficult to dress like a telephone repairman, construction worker, or building inspector and move freely throughout a building. Some might even say that to go almost anywhere in any building, all one really needs is a clipboard and an attitude. If you look as if you have a mission and appear competent, most people will leave you alone. How can organizations combat this type of attack? By requiring that all individuals entering the facility display appropriate visitor badges and be escorted when they are in restricted areas.

Inventory Management

Like other organizational resources, computing equipment should be inventoried and inspected on a regular basis. The management of computer inventory is an important part of physical security. How else can corporate security know if an employee has been pilfering computer supplies or a former employee has taken organizational equipment home? Similarly, classified information should also be inventoried and managed. In the military, whenever a classified document needs to be reproduced, a stamp is placed on the original before it is copied. This stamp states the document's classification level and the text imprint "of " so that the person making the copies can mark the sequence number for each copy as well as the total number of copies being made. If, for example, twenty-five copies are to be made, the person responsible for copying the document writes "26" in the right blank, makes copies, and then numbers them. Why 26 and not 25? The original is always document number one. After the numbering, each classified copy is issued to the assigned person, who signs for it. While this procedure may be overkill for most organizations, it does ensure that the inventory management of classified documents is secure at all times. Also, the formality of having to sign for a document cements its worth in the mind of the recipient.

Selected Readings

- *Effective Physical Security, Third Edition* by Lawrence Fennelly. Butterworth-Heinemann.
- *Build the Best Data Center Facility for Your Business* by Douglas Alger. Cisco Press.
- *Guard Force Management, Updated Edition* by Lucien Canton. Butterworth-Heinemann.

Chapter Summary

- Physical security requires the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization.
- Many threats to information security can also be classified as threats to physical security. An organization's policy should guide the planning for physical security throughout the development life cycle.
- In facilities management, a secure facility is a physical location that has controls to minimize the risk of attacks from physical threats. A secure facility can use natural terrain, traffic flow, and urban development, and can complement these environmental elements with protection mechanisms, such as fences, gates, walls, guards, and alarms.
- The management of keys and locks is a fundamental part of general management's responsibility for the organization's physical environment.
- A fail-safe lock is usually used on an exit door where human safety in the event of a fire or other emergency is the essential consideration. A fail-secure lock is used when human safety is not a factor.
- Monitoring equipment can record events that guards and dogs might miss and can be used in areas where other types of physical controls are not practical.
- Just as with any phase of the security process, the implementation of physical security must be constantly documented, evaluated, and tested; also once the physical security of a facility is established, it must be diligently maintained.
- Fire detection systems are devices that detect and respond to a fire or potential fire. Fire suppression systems stop the progress of a fire once activated.
- There are three basic types of fire detection systems: thermal detection, smoke detection, and flame detection.
- There are four environmental variables controlled by HVAC systems that can cause damage to information-carrying systems: temperature, filtration, humidity, and static electricity.
- Computer systems depend on stable power supplies to function; when power levels are too high, too low, or too erratic, computer circuitry can be damaged or destroyed. The power provided to computing and networking equipment should contain no unwanted fluctuations, and should have no embedded signaling.
- Water problems and the weakening and subsequent failure of a building's physical structure represent potential threats to the safety of people and to the integrity and availability of information assets.
- Data can be intercepted electronically and manually. There are three routes of data interception: direct observation, interception of data transmission, and interception of electromagnetic radiation.
- TEMPEST is a technology that prevents the loss of data that may result from the emission of electromagnetic radiation (EMR).
- With the increased use of laptops, handhelds, and PDAs, organizations should be aware that mobile computing requires even more security than the average in-house system.



- Remote site computing requires a secure extension of the organization's internal networks and special attention to security for any connected home or off-site computing technology.
- Like computing equipment, classified information should also be inventoried and managed. If multiple copies of a classified document are made, they should be numbered and tracked.

Review Questions

1. What is physical security? What are the primary threats to physical security? How are they made manifest in attacks against the organization?
2. What are the roles of IT, security, and general management with regard to physical security?
3. How does physical access control differ from the logical access control described in earlier chapters? How is it similar?
4. Define a secure facility. What is the primary objective of the design of such a facility? What are some of the secondary objectives of the design of a secure facility?
5. Why are guards considered the most effective form of control for situations that require decisive action in the face of unfamiliar stimuli? Why are they usually the most expensive controls to deploy? When should dogs be used for physical security?
6. List and describe the four categories of locks. In which situation is each type of lock preferred?
7. What are the two possible modes that locks use when they fail? What implications do these modes have for human safety? In which situation is each mode preferred?
8. What is a mantrap? When should it be used?
9. What is the most common form of alarm? What does it detect? What types of sensors are commonly used in this type of alarm system?
10. Describe a physical firewall that is used in buildings. List the reasons why an organization might need firewalls for physical security controls.
11. What is considered the most serious threat within the realm of physical security? Why is it valid to consider this threat the most serious?
12. What three elements must be present for a fire to ignite and continue to burn? How do fire suppression systems manipulate the three elements to quell fires?
13. List and describe the three fire detection technologies covered in the chapter. Which is currently the most commonly used?
14. List and describe the four classes of fire described in the text. Does the class of a fire dictate how to control the fire?
15. What is Halon, and why is its use restricted?
16. What is the relationship between HVAC and physical security? What four physical characteristics of the indoor environment are controlled by a properly designed HVAC system? What are the optimal temperature and humidity ranges for computing systems?

17. List and describe the four primary types of UPS systems. Which is the most effective and the most expensive, and why?
18. What two critical functions are impaired when water is not available in a facility? Why are these functions important to the operation of the organization's information assets?
19. List and describe the three fundamental ways that data can be intercepted. How does a physical security program protect against each of these data interception methods?
20. What can you do to reduce the risk of laptop theft?

Exercises

1. Assume that your organization is planning to have a server room that functions without human beings—in other words, the functions are automated (such a room is often called a lights-out server room). Describe the fire control system(s) you would install in that room.
2. Assume that you have converted part of an area of general office space into a server room. Describe the factors you would consider when planning for each of the following:
 - a. Walls and doors
 - b. Physical access control
 - c. Fire detection
 - d. Fire suppression
 - e. Heating, ventilating, and air-conditioning
 - f. Power quality and distribution
3. Assume that you have been asked to review the power needs for a standalone computer system which processes important but noncritical data and does not have to be online at all times, and which stores valuable data that could be corrupted if the power to the system were suddenly interrupted. Which UPS features are most important to such a system? Which type of UPS do you recommend for this system?
4. Using the floor plan of a building you are familiar with, design an electronic monitoring plan that includes closed-circuit television, burglar alarms with appropriate sensors, fire detectors, and fire suppression and physical access controls for key entrances.
5. Define the required wattage for a UPS for the following systems:
 - a. Monitor: 2 amps; CPU: 3 amps; printer: 3 amps
 - b. Monitor: 3 amps; CPU: 4 amps; printer: 3 amps
 - c. Monitor: 3 amps; CPU: 4 amps; printer: 4 amps

Search the Web for a UPS that provides the wattage necessary to run the systems listed above for at least 15 minutes during a power outage.



Case Exercises

Amy walked into her office cubicle and sat down. The entire episode with the blond man had taken well over two hours of her day. Plus, the police officers had told her the district attorney would also be calling to make an appointment to speak to her, which meant she would have to spend even more time dealing with this incident. She hoped her manager would understand.

Questions:

1. Based on this case study, what security awareness and training documents and posters had an impact in this event?
2. Do you think that Amy should have done anything differently? What would you have done in the situation in which she found herself?

Endnotes

1. Parker, Donn B. *Fighting Computer Crime*. New York: John Wiley and Sons Inc., 1998, 250–251.
2. Military-net.com. “General Military Knowledge.” *Military-net.com Online*. Accessed 5 July 2007 from www.military-net.com/education/mpdgeneral.html.
3. Army Study Guide.com. Online. Accessed 5 July 2007 from www.armystudyguide.com/content/army_board_study_guide_topics/guard_duty/guard-duty-study-guide.shtml.
4. Swanson, Marianne. *Guide for Developing Security Plans for Information Technology Systems*. December 1998. National Institute of Standards and Technology SP 800-18, 30. Accessed 5 July 2007 from <http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>.
5. Artim, Nick. *An Introduction to Fire Detection, Alarm, and Automatic Fire Sprinklers*. Emergency Management, Technical Leaflet 2, sec. 3. Middlebury: Fire Safety Network.
6. Environmental Protection Agency. “Halon Substitutes Under SNAP as of 21 August 2003.” *EPA Online*. Accessed 5 July 2007 from www.epa.gov/ozone/snap/fire/halo.pdf.
7. Ibid.
8. Webopedia. “Static Electricity and Computers.” *Webopedia Online*. May 2003. Accessed 7 July 2007 from www.webopedia.com/DidYouKnow/Computer_Science/2002/static.asp.
9. Kozierok, Charles M. “Uninterruptible Power Supply Types.” *PC Guide Online*. 17 April 2001. Accessed 5 July 2007 from www.pcguides.com/ref/power/ext/ups/types.htm.
10. Van Eck, Wim. “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?” *Computers & Security* 4 (1985): 269–286.

11. Loughry, Joe, and Umphress, David A. "Information Leakage from Optical Emanations." *ACM Transactions on Information and System Security* 7, no. 7, accepted March 2002.
12. PC Privacy. "Is Tempest a Threat or Hoax?" *PC Privacy* 8, no. 4 (April 2000).
13. Metropolitan Police of the District of Columbia. "Tips for Preventing Laptop Computer Theft." *Government of The District of Columbia Online*. Accessed 7 July 2007 from http://mpdc.dc.gov/mpdc/cwp/view,a,1237,q,543203,mpdcNav_GID,1548.asp.

