Physical and Environmental Security

This chapter presents the following:
- Administrative, technical, and physical controls
- Facility location, construction, and management
- Physical security risks, threats, and countermeasures
- Electric power issues and countermeasures
- Fire prevention, detection, and suppression
- Intrusion detection systems

Security is very important to organizations and their infrastructures, and physical security is no exception. Hacking is not the only way information and their related systems can be compromised. Physical security encompasses a different set of threats, vulnerabilities, and risks than the other types of security we’ve addressed so far. Physical security mechanisms include site design and layout, environmental components, emergency response readiness, training, access control, intrusion detection, and power and fire protection. Physical security mechanisms protect people, data, equipment, systems, facilities, and a long list of company assets.

Introduction to Physical Security

The physical security of computers and their resources in the 1960s and 1970s was not as challenging as it is today because computers were mostly mainframes that were locked away in server rooms, and only a handful of people knew what to do with them anyway. Today, a computer sits on almost every desk in every company, and access to devices and resources is spread throughout the environment. Companies have several wiring closets and server rooms, and remote and mobile users take computers and resources out of the facility. Properly protecting these computer systems, networks, facilities, and employees has become an overwhelming task to many companies.

Theft, fraud, sabotage, vandalism, and accidents are raising costs for many companies because environments are becoming more complex and dynamic. Security and
complexity are at the opposite ends of the spectrum. As environments and technology become more complex, more vulnerabilities are introduced that allow for compromises to take place. Most companies have had memory or processors stolen from workstations, while some have had computers and laptops taken. Even worse, many companies have been victims of more dangerous crimes, such as robbery at gunpoint, a shooting rampage by a disgruntled employee, anthrax, bombs, and terrorist activities. Many companies may have implemented security guards, closed-circuit TV (CCTV) surveillance, intrusion detection systems (IDSs), and requirements for employees to maintain a higher level of awareness of security risks. These are only some of the items that fall within the physical security boundaries. If any of these does not provide the necessary protection level, it could be the weak link that causes potentially dangerous security breaches.

Most people in the information security field do not think as much about physical security as they do about computer security and the associated hackers, ports, viruses, and technology-oriented security countermeasures. But information security without proper physical security could be a waste of time.

Even people within the physical security market do not always have a holistic view of physical security. There are so many components and variables to understand, people have to specialize in specific fields, such as secure facility construction, risk assessment and analysis, secure data center implementation, fire protection, IDS and CCTV implementation, personnel emergency response and training, legal and regulatory aspects of physical security, and so on. Each has its own focus and skill set, but for an organization to have a solid physical security program, all of these areas must be understood and addressed.

Just as most software is built with functionality as the number one goal, with security somewhere farther down the priority list, many facilities and physical environments are built with functionality and aesthetics in mind, with not as much concern for providing levels of protection. Many thefts and deaths could be prevented if all organizations were to implement physical security in an organized, mature, and holistic manner. Most people are not aware of many of the crimes that happen every day. Many people also are not aware of all the civil lawsuits that stem from organizations not practicing due diligence and due care pertaining to physical security. The following is a short list of some examples of things companies are sued for pertaining to improper physical security implementation and maintenance:

- An apartment complex does not respond to a report of a broken lock on a sliding glass door and subsequently a woman who lives in that apartment is raped by an intruder.
- Bushes are growing too close to an ATM, allowing criminals to hide behind them and attack individuals as they withdraw money from their accounts.
- A portion of an underground garage is unlit, which allows an attacker to sit and wait for an employee who works late.
- A gas station’s outside restroom has a broken lock, which allows an attacker to enter after a female customer and kill her.
Chapter 6: Physical and Environmental Security

403

A convenience store hangs too many advertising signs and posters on the exterior windows, prompting thieves to choose this store because the signs hide any crimes taking place inside the store from people driving or walking by.

Many examples like this take place every day. These crimes might make it to our local news stations, but there are too many incidents to be reported in national newspapers or on network news. It is important as a security professional to evaluate security from the standpoint of a potential criminal, and to detect and remedy any points of vulnerability that could be exploited by the same. Similar to how so many people are unaware of many of these “smaller” crimes that happen every day, they are also unaware of all the civil suits brought about because organizations are not practicing due diligence and due care regarding physical security. While many different examples of this occur every day, these kinds of crimes may never make the news because they are either overshadowed by larger news events or there are just too many of them to all be reported on. A security professional needs to regard security as a holistic process and as such it must be viewed from all angles and approaches. Because danger can come from anywhere and take any different number of shapes, formats, and levels of severity.

Physical security has a different set of vulnerabilities, threats, and countermeasures from that of computer and information security. The set for physical security has more to do with physical destruction, intruders, environmental issues, theft, and vandalism. When security professionals look at information security, they think about how someone can enter an environment in an unauthorized manner through a port, modem, or wireless access point. When security professionals look at physical security, they are concerned with how people can physically enter an environment and cause an array of damages.

The threats that an organization faces fall into many different categories:

- **Natural environmental threats** Floods, earthquakes, storms and tornadoes, fires, extreme temperature conditions, and so forth
- **Supply system threats** Power distribution outages, communications interruptions, and interruption of other natural energy resources such as water, steam, and gas, and so on
- **Manmade threats** Unauthorized access (both internal and external), explosions, damage by angry employees, employee errors and accidents, vandalism, fraud, theft, and others
- **Politically motivated threats** Strikes, riots, civil disobedience, terrorist attacks and bombings, and so forth

In all situations, the primary consideration, above all else, is that nothing should impede **life safety** goals. When we discuss life safety, protecting human life is first priority. Good planning helps balance life safety concerns and other security measures. For example, barring a door to prevent unauthorized physical intrusion might prevent individuals from being able to escape in the event of a fire.

---

**NOTE** Life safety goals should always take precedence over all other types of goals.
A physical security program should comprise safety and security mechanisms. Safety deals with the protection of life and assets against fire, natural disasters, and devastating accidents. Security addresses vandalism, theft, and attacks by individuals. Many times an overlap occurs between the two, but both types of threat categories must be understood and properly planned for. This chapter addresses both safety and security mechanisms that every security professional should be aware of.

Physical security must be implemented based on a *layered defense model*, which means that physical controls should work together in a tiered architecture. The concept is that if one layer fails, other layers will protect the valuable asset. Layers would be implemented moving from the perimeter toward the asset. For example, you would have a fence, then your facility walls, then an access control card device, then a guard, then an IDS, and then locked computer cases and safes. This series of layers will protect the company’s most sensitive assets, which would be placed in the innermost control zone of the environment. So if the bad guy were able to climb over your fence and outsmart the security guard, he would still have to circumvent several layers of controls before getting to your precious resources and systems.

Security needs to protect all the assets of the organization and enhance productivity by providing a secure and predictable environment. Good security enables employees to focus on their tasks at hand, and encourages attackers to move on to a more vulnerable and easier target. This is the hope, anyway. Keeping in mind the AIC security triad that has been presented in previous chapters, we look at physical security that can affect the *availability* of company resources, the *integrity* of the assets and environment, and the *confidentiality* of the data and business processes.

**The Planning Process**

*Okay, so what are we doing and why?*

*Response: We have no idea.*

A designer, or team of designers, needs to be identified to create or improve upon an organization’s current physical security program. The team must work with management to define the objectives of the program, design the program, and develop performance-based metrics and evaluation processes to ensure the objectives are continually being met.

The objectives of the physical security program depend upon the level of protection required for the various assets and the company as a whole. And this required level of protection, in turn, depends upon the organization’s acceptable risk level. This acceptable risk level should be derived from the laws and regulations with which the organization must comply and from the threat profile of the organization overall. This requires identifying who and what could damage business assets, identifying the types of attacks and crimes that could take place, and understanding the business impact of these threats. The type of physical countermeasures required and their adequacy or inadequacy needs to be measured against the organization’s threat profile. A financial institution has a much different threat profile, and thus a much different acceptable risk level, when compared to a grocery store. The threat profile of a hospital is different from the...
threat profile of a military base or a government agency. The team must understand the
types of adversaries it must consider, the capabilities of these adversaries, and the re-
sources and tactics these individuals would use. (Review Chapter 3 for a discussion of
acceptable risk level concepts.)

Physical security is a combination of people, processes, procedures, and equipment
to protect resources. The design of a solid physical security program should be me-
thodical and weigh the objectives of the program and the available resources. Although
every organization is different, the approach to constructing and maintaining a physi-
cal security program is the same. The organization must first define the vulnerabilities,
threats, threat agents, and targets.

NOTE

Remember that a vulnerability is a weakness and a threat is the
potential that someone will identify this weakness and use it against you. The
threat agent is the person or mechanism that actually exploits this identified
vulnerability.

Threats must be broken down into different categories, such as internal and exter-
nal threats. Inside threats may include misbehaving devices, fire hazards, or internal
employees who aim to damage the company in some way. Internal employees have
intimate knowledge of the company’s facilities and assets, which is usually required to
perform tasks and responsibilities—but this makes it easier for the insider to carry out
damaging activity without being noticed. Unfortunately, a large threat to companies
can be their own security guards, which is usually not realized until it is too late. These
people have keys and access codes to all portions of a facility and usually work during
employee off-hours. This gives the guards ample windows of opportunity to carry out
their crimes. It is critical for a company to carry out a background investigation, or pay
a company to perform this service, before hiring a security guard. If you hire a wolf to
guard the chicken coop, things can get ugly.

External threats come in many different forms as well. Government buildings are usu-
ally chosen targets for some types of political revenge. If a company performs abortions
or conducts animal research, then activists are usually a large and constant threat. And, of
course, banks and armored cars are tempting targets for organized crime members.

A threat that is even trickier to protect against is collusion, in which two or more
people work together to carry out fraudulent activity. Many criminal cases have uncov-
ered insiders working with outsiders to defraud or damage a company. The types of
controls for this type of activity are procedural protection mechanisms, which were
described at length in Chapter 3. This may include separation of duties, pre-employ-
ment background checks, rotations of duties, and supervision.

As with any type of security, most attention and awareness surrounds the exciting
and headline-grabbing tidbits about large crimes being carried out and criminals being
captured. In information security, most people are aware of viruses and hackers but not
the components that make up a corporate security program. The same is true for physi-
cal security. Many people talk about current robberies, murders, and other criminal
activity at the water cooler but do not pay attention to the necessary framework that
should be erected and maintained to reduce these types of activities. An organization’s physical security program should address the following goals:

- **Crime and disruption prevention through deterrence**  Fences, security guards, warning signs, and so forth
- **Reduction of damage through the use of delaying mechanisms**  Layers of defenses that slow down the adversary, such as locks, security personnel, barriers
- **Crime or disruption detection**  Smoke detectors, motion detectors, CCTV, and so forth
- **Incident assessment**  Response of security guards to detected incidents and determination of damage level
- **Response procedures**  Fire suppression mechanisms, emergency response processes, law enforcement notification, consultation with outside security professionals

So, an organization should try to prevent crimes and disruptions from taking place, but must also plan to deal with them when they do happen. A criminal should be delayed in her activities by having to penetrate several layers of controls before gaining access to a resource. All types of crimes and disruptions should be able to be detected through components that make up the physical security program. Once an intrusion is discovered, a security guard should be called upon to assess the situation. The security guard must then know how to properly respond to a large range of potentially dangerous activities. The emergency response activities could be carried out by the organization’s internal security team or by outside experts.

This all sounds straightforward enough, until the team responsible for developing the physical security program looks at all the possible threats, the finite budget that the team has to work with, and the complexity of choosing the right combination of countermeasures and ensuring that they all work together in a manner that ensures no gaps

---

**The Commission on Critical Infrastructure Protection**

In Chapter 2, we looked at the President’s Commission on Critical Infrastructure Protection (PCCIP), which requires organizations that are part of the national critical infrastructure to have adequate protection mechanisms in place. Although this executive order deals with technical protection of systems and data, it also deals with physical protection of the facilities themselves. It outlines that power systems, emergency services, water supply systems, gas and oil transportation, and government services must be evaluated to ensure proper physical security is implemented. It really does not make a lot of sense to ensure that hackers can’t get to your server if you don’t also ensure that someone can’t just walk in and steal it.

Legislation passed over the last few years has increased the emphasis on protecting facilities that use or produce biological and chemical agents against terrorist acts.
of protection. All of these components must be understood in depth before the design of a physical security program can begin.

As with all security programs, it is possible to determine how beneficial and effective your physical security program is only if it is monitored through a performance-based approach. This means you should devise measurements and metrics to measure the effectiveness of the chosen countermeasures. This enables management to make informed business decisions when investing in the protection of the organization’s physical security. The goal is to increase the performance of the physical security program and decrease the risk to the company in a cost-effective manner. You should establish a baseline of performance and thereafter continually evaluate performance to make sure that the company’s protection objectives are being met. The following provides some examples of possible performance metrics:

- Number of successful crimes
- Number of successful disruptions
- Number of unsuccessful crimes or disruptions
- Time between detection, assessment, and recovery steps
- Business impact of disruptions
- Number of false-positive detection alerts
- Time it took for a criminal to defeat a control
- Time it took to restore the operational environment

Capturing and monitoring these types of metrics enables the organization to identify deficiencies, evaluate improvement measures, and perform cost/benefit analyses.

The physical security team needs to carry out a risk analysis, which will identify the organization’s vulnerabilities, threats, and business impacts. The team should present these findings to management and work with them to define an acceptable risk level for the physical security program. From there, the team must develop baselines (minimum levels of security) and metrics in order to evaluate and determine if the baselines are being met by the implemented countermeasures. Once the team identifies and implements the countermeasures, the performance of these countermeasures should be continually evaluated and expressed in the previously created metrics. These performance values are compared to the set baselines. If the baselines are continually maintained, then the security program is successful, because the company’s acceptable risk level is not being exceeded. This is illustrated in Figure 6-1.

So, before an effective physical security program can be rolled out, the following steps must be taken:

- Identify a team of internal employees and/or external consultants who will build the physical security program through the following steps.
- Carry out a risk analysis to identify the vulnerabilities and threats and calculate the business impact of each threat.
- Work with management to define an acceptable risk level for the physical security program.
Derive the required performance baselines from the acceptable risk level.

Create countermeasure performance metrics.

Develop criteria from the results of the analysis, outlining the level of protection and performance required for the following categories of the security program:

- Deterrence
- Delaying
- Detection
- Assessment
- Response

Identify and implement countermeasures for each program category.

Continuously evaluate countermeasures against the set baselines to ensure the acceptable risk level is not exceeded.

Once these steps have taken place (or continue to take place, as in the case of the last step), then the team is ready to move forward in its actual design phase. The design will incorporate the controls required for each category of the program; deterrence, delaying, detection, assessment, and response. We will dig deeper into these categories and their corresponding controls later in the chapter in the “Designing a Physical Security Program” section.

One of the most commonly used approaches in physical security program development is described in the following section.
Crime Prevention Through Environmental Design

This place is so nice and pretty and welcoming. No one would want to carry out crimes here.

Crime Prevention Through Environmental Design (CPTED) is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior. It provides guidance in loss and crime prevention through proper facility construction and environmental components and procedures.

CPTED concepts were developed in the 1960s. They have been built upon and have matured as our environments and crime types have evolved. CPTED has been used not just to develop corporate physical security programs, but also for large-scale activities such as development of neighborhoods, towns, and cities. It addresses landscaping, entrances, facility and neighborhood layouts, lighting, road placement, and traffic circulation patterns. It looks at microenvironments, such as offices and restrooms, and macroenvironments, like campuses and cities. The crux of CPTED is that the physical environment can be manipulated to create behavioral effects that will reduce crime and the fear of crime. It looks at the components that make up the relationship between humans and their environment. This encompasses the physical, social, and psychological needs of the users of different types of environments and predictable behaviors of these users and offenders.

CPTED provides guidelines on items some of us might not consider. For example, hedges and planters around a facility should not be higher than 2.5 feet tall, so they cannot be used to gain access to a window. A data center should be located at the center of a facility, so the facility’s walls will absorb any damages from external forces, instead of the data center. Street furnishings (benches and tables) encourage people to sit and watch what is going on around them, which discourages criminal activity. A corporation’s landscape should not include wooded areas or other places where intruders can hide. Ensure that CCTV cameras are mounted in full view, so criminals know their activities will be captured and other people know the environment is well monitored and thus safer.

Similarities in Approaches

The risk analysis steps are very similar to the steps outlined in Chapter 3 for the development of an organizational security program and the steps outlined in Chapter 9 for a business impact analysis, because each of these processes (development of an information security program, a physical security program, or a business continuity plan) accomplishes goals that are similar to the goals of the other two processes, but with different focuses. Each process requires a team to carry out a risk analysis, to determine the company’s threats and risks. An information security program looks at the internal and external threats to resources and data through business processes and technological means. Business continuity looks at how natural disasters and disruptions could damage the organization, while physical security looks at internal and external physical threats to the company resources.

Each requires a solid risk analysis process. Review Chapter 3 to understand the core components of every risk analysis.
CPTED and target hardening are two different approaches. **Target hardening** focuses on denying access through physical and artificial barriers (alarms, locks, fences, and so on). Traditional target hardening can lead to restrictions on the use, enjoyment, and aesthetics of an environment. Sure, we can implement hierarchies of fences, locks, and intimidating signs and barriers—but how pretty would that be? If your environment is a prison, this look might be just what you need. But if your environment is an office building, you’re not looking for Fort Knox décor. Nevertheless, you still must provide the necessary levels of protection, but your protection mechanisms should be more subtle and unobtrusive.

Let’s say your organization’s team needs to protect a side door at your facility. The traditional target-hardening approach would be to put locks, alarms, and cameras on the door, install an access control mechanism, such as a proximity reader, and instruct security guards to monitor this door. The CPTED approach would be to ensure there is no sidewalk leading to this door from the front of the building if you don’t want customers using it. The CPTED approach would also ensure no tall trees or bushes block the ability to view someone using this door. Barriers such as trees and bushes may make intruders feel more comfortable in attempting to break in through a secluded door.

The best approach is usually to build an environment from a CPTED approach and then apply the target-hardening components on top of the design where needed.

If a parking garage was developed using the CPTED approach, the stair towers and elevators within the garage may have glass windows instead of metal walls, so people feel safer and potential criminals will not carry out crimes in this more visible environment. Pedestrian walkways would be created such that people could look out across the rows of cars and see any suspicious activities. The different rows for cars to park in would be separated by low walls and structural pillars, instead of solid walls, to allow pedestrians to view activities within the garage.

CPTED provides three main strategies to bring together the physical environment and social behavior to increase overall protection: natural access control, natural surveillance, and territorial reinforcement.

**Natural Access Control**

Natural access control is the guidance of people entering and leaving a space by the placement of doors, fences, lighting, and even landscaping. For example, an office building may have external bollards with lights in them, as shown in Figure 6-2. These bollards actually carry out different safety and security services. The bollards themselves protect the facility from physical destruction by preventing people from driving their cars into the building. The light emitted helps ensure that criminals do not have a dark place to hide. And the lights and bollard placement guides people along the sidewalk to the entrance, instead of using signs or railings. As shown in Figure 6-2, the landscape, sidewalks, lighted bollards, and clear sight lines are used as natural access controls.
They work together to give individuals a feeling of being in a safe environment and help dissuade criminals by working as deterrents.

**NOTE** Bollards are short posts commonly used to prevent vehicular access and to protect a building or people walking on a sidewalk from vehicles. They can also be used to direct foot traffic.

Clear lines of sight and transparency can be used to discourage potential offenders, because of the visible absence of places to hide or carry out criminal activities.

The CPTED model shows how security zones can be created. An environment’s space should be divided into zones with different security levels, depending upon who needs to be in that zone and the associated risk. The zones can be labeled as controlled, restricted, public, or sensitive. This is conceptually similar to information classification, as described in Chapter 3. In a data classification program, different classifications are created, along with data handling procedures and the level of protection that each classification requires. The same is true of physical zones. Each zone should have a specific...
protection level required of it, which will help dictate the types of controls that should be put into place.

Access control should be in place to control and restrict individuals from going from one security zone to the next. Access control should also be in place for all facility entrances and exits. The security program development team needs to consider other ways in which intruders can gain access to buildings, such as by climbing adjacent trees to access skylights, upper-story windows, and balconies. The following controls are commonly used for access controls within different organizations:

- Limit the number of entry points.
- Force all guests to go to a front desk and sign in before entering the environment.
- Reduce the number of entry points even further after hours or during the weekend when not as many employees are around.
- Have a security guard validate a picture ID before allowing entrance.
- Require guests to sign in and be escorted.
- Encourage employees to question strangers.

Access barriers can be naturally created (cliffs, rivers, hills), existing manmade elements (railroad tracks, highways), or artificial forms designed specifically to impede movement (fences, closing streets).
Natural Surveillance
Surveillance can also take place through organized means (security guards), mechanical means (CCTV), and natural strategies (straight lines of sight, low landscaping, raised entrances). The goal of natural surveillance is to make criminals feel uncomfortable by providing many ways observers could potentially see them, and make all other people feel safe and comfortable, by providing an open and well-designed environment.

Natural surveillance is the use and placement of physical environmental features, personnel walkways, and activity areas in ways that maximize visibility. Figure 6-3 illustrates a stairway in a parking garage designed to be open and allow easy observation.

Territorial Reinforcement
The third CPTED strategy is territorial reinforcement, which creates physical designs that emphasize or extend the company’s physical sphere of influence so legitimate users feel a sense of ownership of that space. Territorial reinforcement can be implemented through the use of walls, fences, landscaping, light fixtures, flags, clearly marked addresses, and decorative sidewalks. The goal of territorial reinforcement is to create a sense of a dedicated community. Companies implement these elements so employees

Figure 6-3  Open areas reduce the likelihood of criminal activity.
feel proud of their environment and have a sense of belonging, which they will defend if required to do so. These elements are also implemented to give potential offenders the impression that they do not belong there, that their activities are at risk of being observed, and that their illegal activities will not be tolerated or ignored.

Most corporate environments use a mix of the CPTED and target-hardening approaches. CPTED deals mainly with the construction of the facility, its internal and external designs, and exterior components such as landscaping and lighting. If the environment is built based on CPTED, then the target hardening is like icing on the cake. The target-hardening approach applies more granular protection mechanisms, such as locks and motion detectors. The rest of the chapter looks at physical controls that can be used in both models.

Designing a Physical Security Program

Our security guards should wear pink uniforms and throw water balloons at intruders. Response: Very scary environment indeed!

If a team is organized to assess the protection level of an existing facility, it needs to investigate the following:

- HVAC systems
- Construction materials of walls and ceilings
- Power distribution systems
- Communication paths and types (copper, telephone, fiber)
- Surrounding hazardous materials
- Exterior components:
  - Topography
  - Proximity to airports, highways, railroads
  - Potential electromagnetic interference from surrounding devices
  - Climate
  - Soil
  - Existing fences, detection sensors, cameras, barriers
  - Working hours of employees
  - Operational activities that depend upon physical resources
  - Vehicle activity
  - Neighbors

To properly obtain this information, the team should do surveys and interview various employees. All of this collected data will help the team to evaluate the current controls, identify weaknesses, and ensure operational productivity is not negatively affected by implementing new controls.

Although there are usually written policies and procedures on what should be taking place pertaining to physical security, policies and reality do not always match up. It is
important for the team to observe how the facility is used, note daily activities that could introduce vulnerabilities, and determine how the facility is protected. This information should be documented and compared to the information within the written policy and procedures. In most cases, existing gaps must be addressed and fixed. Just writing out a policy helps no one if it is not actually followed.

Every organization must comply with various regulations, whether they be safety and health regulations, fire codes, state and local building codes, Departments of Defense, Energy, or Labor requirements, or some other agency’s regulations. The organization may also have to comply with requirements of the Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA), if it is operating in the United States, or with the requirements of equivalent organizations within another country. The physical security program development team must understand all the regulations the organization must comply with and how to reach compliance through physical security and safety procedures.

Legal issues must be understood and properly addressed, also. These issues may include access availability for the disabled, liability issues, the failure to protect assets and people, excessive force used by security guards, and so on. This long laundry list of items can get a company into legal trouble if it is not doing what it is supposed to. Occasionally, the legal trouble may take the form of a criminal case—for example, if doors default to being locked when power is lost and, as a result, several employees are trapped and killed during a fire, criminal negligence may be alleged. Legal trouble can also come in the form of civil cases—for instance, if a company does not remove the ice on its sidewalks and a pedestrian falls and breaks his ankle, the pedestrian may sue the company. The company may be found negligent and held liable for damages.

Every organization should have a facility safety officer, whose main job is to understand all the components that make up the facility and what the company needs to do to protect its assets and stay within compliance. This person should oversee facility management duties day in and day out, but should also be heavily involved with the team that has been organized to evaluate the organization’s physical security program.

A physical security program is a collection of controls that are implemented and maintained to provide the protection levels necessary to be in compliance with the physical security policy. The policy should embody all the regulations and laws that must be adhered to and should set the risk level the company is willing to accept.

Activity Support
CPTED also encourages activity support, which is planned activities for the areas to be protected. These activities are designed to get people to work together to increase the overall awareness of acceptable and unacceptable activities in the area. The activities could be neighborhood watch groups, company barbeques, block parties, or civic meetings. This strategy is sometimes the reason for particular placement of basketball courts, soccer fields, or baseball fields in open parks. The increased activity will hopefully keep the bad guys from milling around doing things the community does not welcome.
By this point, the team has carried out a risk analysis, which consisted of identifying the company's vulnerabilities, threats, and business impact pertaining to the identified threats. The program design phase should begin with a structured outline, which will evolve into a framework. This framework will then be fleshed out with the necessary controls and countermeasures. The outline should contain the program categories and the necessary countermeasures. The following is a simplistic example:

I. Deterrence of criminal activity
   A. Fences
   B. Warning signs
   C. Security guards
   D. Dogs

II. Delay of intruders to help ensure they can be caught
   A. Locks
   B. Defense-in-depth measures
   C. Access controls

III. Detection of intruders
   A. External intruder sensors
   B. Internal intruder sensors

IV. Assessment of situations
   A. Security guard procedures
   B. Communication structure (calling tree)

V. Response to intrusions and disruptions
   A. Response force
   B. Emergency response procedures
   C. Police, fire, medical personnel

The team can then start addressing each phase of the security program, usually starting with the facility.

**Facility**

*I can't see the building.*

*Response: That's the whole idea.*

When a company decides to erect a building, it should consider several factors before pouring the first batch of concrete. Of course, land prices, customer population, and marketing strategies are reviewed, but as security professionals, we are more interested in the confidence and protection that a specific location can provide. Some organizations that deal with top-secret or confidential information make their facilities unnoticeable so they do not attract the attention of would-be attackers. The building may be hard to see from the surrounding roads, the company signs and logos may be small and not easily noticed, and the markings on the building may not give away any
information that pertains to what is going on inside that building. It is a type of urban camouflage that makes it harder for the enemy to seek out that company as a target.

A company should evaluate how close the facility would be to a police station, fire station, and medical facilities. Many times, the proximity of these entities raises the real estate value of properties, but for good reason. If a chemical company that manufactures highly explosive materials needs to build a new facility, it may make good business sense to put it near a fire station. (Although the fire station might not be so happy.) If another company that builds and sells expensive electronic devices is expanding and needs to move operations into another facility, police reaction time may be looked at when choosing one facility location over another. Each of these issues—police station, fire station, and medical facility proximity—can also reduce insurance rates and must be looked at carefully. Remember that the ultimate goal of physical security is to ensure the safety of personnel. Always keep that in mind when implementing any sort of physical security control. Protect your fellow humans, be your brother’s keeper, and then run.

Some buildings are placed in areas surrounded by hills or mountains to help prevent eavesdropping of electrical signals emitted by the facility’s equipment. In some cases, the organization itself will build hills or use other landscaping techniques to guard against eavesdropping. Other facilities are built underground or right into the side of a mountain for concealment and disguise in the natural environment, and for protection from radar tools, spying activities, and aerial bomb attacks.

**Issues with Selecting a Facility Site**

When selecting a location for a facility, some of the following items are critical to the decision-making process:

- **Visibility**
  - Surrounding terrain
  - Building markings and signs
  - Types of neighbors
  - Population of the area
- **Surrounding area and external entities**
  - Crime rate, riots, terrorism attacks
  - Proximity to police, medical, and fire stations
  - Possible hazards from surrounding area
- **Accessibility**
  - Road access
  - Traffic
  - Proximity to airports, train stations, and highways
- **Natural disasters**
  - Likelihood of floods, tornadoes, earthquakes, or hurricanes
  - Hazardous terrain (mudslides, falling rock from mountains, or excessive snow or rain)
Construction

We need a little more than glue, tape, and a stapler.

Physical construction materials and structure composition need to be evaluated for their appropriateness to the site environment, their protective characteristics, their utility, and their costs and benefits. Different building materials provide different levels of fire protection and have different rates of combustibility, which correlate with their fire ratings. When making structural decisions, the decision of what type of construction material to use (wood, concrete, or steel) needs to be considered in light of what the building is going to be used for. If an area is going to be used to store documents and old equipment, it has far different needs and legal requirements than if it is going to be used for employees to work in every day.

The load (how much weight that can be held) of a building's walls, floors, and ceilings needs to be estimated and projected to ensure the building will not collapse in different situations. In most cases, this may be dictated by local building codes. The walls, ceilings, and floors must contain the necessary materials to meet the required fire rating and to protect against water damage. The windows (interior and exterior) may need to provide ultraviolet (UV) protection, may need to be shatterproof, or may need to be translucent or opaque, depending on the placement of the window and the contents of the building. The doors (exterior and interior) may need to have directional openings, have the same fire rating as the surrounding walls, prohibit forcible entries, display emergency egress markings, and, depending on placement, have monitoring and attached alarms. In most buildings, raised floors are used to hide and protect wires and pipes, but in turn the floors' outlets need to be electrically grounded because they are raised.

Building codes may regulate all of these issues, but there are still many options within each category that the physical security program development team should review for extra security protection. The right options should accomplish the company's security and functionality needs and still be cost-effective.

When designing and building a facility, the following major items need to be addressed from a physical security point of view:

- **Walls**
  - Combustibility of material (wood, steel, concrete)
  - Fire rating
  - Reinforcements for secured areas

- **Doors**
  - Combustibility of material (wood, pressed board, aluminum)
  - Fire rating
  - Resistance to forcible entry
  - Emergency marking
  - Placement
  - Locked or controlled entrances
  - Alarms
Chapter 6: Physical and Environmental Security

Ground

If you are holding a power cord that has two skinny metal pieces and one fatter, rounder metal piece, which all go into the outlet—what is that fatter, rounder piece for? It is a ground connector, which is supposed to act as the conduit for any excess current to ensure that people and devices are not negatively affected by a spike in electrical current. So, in the wiring of a building, where do you think this ground should be connected? Yep, to the ground. Old mother earth. But many buildings are not wired properly and the ground connector is connected to nothing. This can be very dangerous, since the extra current has nowhere to escape but into our equipment or ourselves.

- Secure hinges
- Directional opening
- Electric door locks that revert to an unlocked state for safe evacuation in power outages
- Type of glass—shatterproof or bulletproof glass requirements

Ceilings

- Combustibility of material (wood, steel, concrete)
- Fire rating
- Weight-bearing rating
- Drop-ceiling considerations

Windows

- Translucent or opaque requirements
- Shatterproof
- Alarms
- Placement
- Accessibility to intruders

Flooring

- Weight-bearing rating
- Combustibility of material (wood, steel, concrete)
- Fire rating
- Raised flooring (electrical grounding)
- Nonconducting surface and material

Heating, ventilation, and air conditioning

- Positive air pressure
- Protected intake vents
- Dedicated power lines
Emergency shutoff valves and switches
Place

Electric power supplies
- Backup and alternate power supplies
- Clean and steady power source
- Dedicated feeders to required areas
- Placement and access to distribution panels and circuit breakers

Water and gas lines
- Shutoff valves—labeled and brightly painted for visibility
- Positive flow (material flows out of building, not in)
- Placement—properly located and labeled

Fire detection and suppression
- Placement of sensors and detectors
- Placement of suppression systems
- Type of detectors and suppression agents

The risk analysis results will help the team determine the type of construction material that should be used when constructing a new facility. Several grades of building construction are available. For example, light frame construction material provides the least amount of protection against fire and forcible entry attempts. It is composed of untreated lumber that would be combustible during a fire. Light frame construction material is usually used to build homes, primarily because it is cheap but also because homes typically are not under the same types of fire and intrusion threats that office buildings are.

Heavy timber construction material is commonly used for office buildings. Combustible lumber is still used in this type of construction, but there are requirements on the thickness and composition of the materials to provide more protection from fire. The construction materials must be at least four inches in thickness. More dense woods are used and are fastened with metal bolts and plates. Whereas light frame construction material has a fire survival rate of 30 minutes, the heavy timber construction material has a fire rate of one hour.

A building could be made up of incombustible material, such as steel, which provides a higher level of fire protection than the previously mentioned materials but loses its strength under extreme temperatures, something that may cause the building to collapse. So, although the steel will not burn, it may melt and weaken. If a building consists of fire-resistant material, the construction material is fire-retardant and has steel rods encased inside of concrete walls and support beams. This provides the most protection against fire and forced entry attempts.

The team should choose its construction material based on the identified threats of the organization and the fire codes to be complied with. If a company is just going to have some office workers in a building and has no real adversaries interested in destroying the facility, then the light frame or heavy timber construction material would be used. Facilities for government organizations, which are under threat by domestic and
foreign terrorists, would be built with fire-resistant materials. A financial institution would also use fire-resistant and reinforcement material within its building. This is especially true for its exterior walls, through which thieves may attempt to drive vehicles to gain access to the vaults.

Calculations of approximate penetration times for different types of explosives and attacks are based on the thickness of the concrete walls and the gauge of rebar used. (Rebar refers to the steel rods encased within the concrete.) So even if the concrete can be damaged, it will take longer to actually cut or break through the rebar. Using thicker rebar and properly placing it within the concrete provides even more protection.

Reinforced walls, rebar, and the use of double walls can be used as delaying mechanisms. The idea is that it will take the bad guy longer to get through two reinforced walls, which gives the response force sufficient time to arrive at the scene and stop the attacker, we hope.

**Entry Points**

Understanding the company needs and types of entry points for a specific building is critical. The various types of entry points may include doors, windows, roof access, fire escapes, chimneys, and service delivery access points. Second and third entry points must also be considered, such as internal doors that lead into other portions of the building and to exterior doors, elevators, and stairwells. Windows at the ground level should be fortified, because they could be easily broken. Fire escapes, stairwells to the roof, and chimneys are many times overlooked as potential entry points.

**NOTE** Ventilation ducts and utility tunnels can also be used by intruders and thus must be properly protected with sensors and access control mechanisms.

The weakest portion of the structure, usually its doors and windows, will likely be attacked first. With regard to doors, the weaknesses usually lie within the frames, hinges, and door material. The bolts, frames, hinges, and material that make up the door should all provide the same level of strength and protection. For example, if a company implements a heavy, nonhollow steel door but uses weak hinges that could be easily extracted, the company is just wasting money. The attacker can just remove the hinges and remove this strong and heavy door.

The door and surrounding walls and ceilings should also provide the same level of strength. If another company has an extremely fortified and secure door but the surrounding wall materials are made out of regular light frame wood, then it is also wasting money on doors. There is no reason to spend a lot of money on one countermeasure that can be easily circumvented by breaking a weaker countermeasure in the same proximity.

**Doors** Different door types for various functionalities include the following:

- Vault doors
- Personnel doors
- Industrial doors
- Vehicle access doors
- Bullet-resistant doors
Doors can be hollow-core or solid-core. The team needs to understand the various entry types and the potential forced-entry threats, which will help them determine what type of door should be implemented. Hollow-core doors can be easily penetrated by kicking or cutting them; thus, they are usually used internally. The team also has a choice of solid-core doors, which are made up of various materials to provide different fire ratings and protection from forced entry. As stated previously, the fire rating and protection level of the door needs to match the fire rating and protection level of the surrounding walls.

Bulletproof doors are also an option if there is a threat that damage could be done to resources by shooting through the door. These types of doors are constructed in a manner that involves sandwiching bullet-resistant and bulletproof material between wood or steel veneers to still give the door some aesthetic qualities while providing the necessary levels of protection.

Hinges and strike plates should be secure, especially on exterior doors or doors used to protect sensitive areas. The hinges should have pins that cannot be removed, and the door frames must provide the same level of protection as the door itself.

Fire codes dictate the number and placement of doors with panic bars on them. These are the crossbars that release an internal lock to allow a locked door to open. Panic bars can be on regular entry doors and also emergency exit doors. Those are the ones that usually have the sign that indicates the door is not an exit point and that an alarm will go off if opened. It might seem like fun and a bit tempting to see if the alarm will really go off or not—but don’t try it. You’re just asking for lots of yelling and dirty looks from the facility management group.

Mantraps and turnstiles can be used so unauthorized individuals entering a facility cannot get in or out if it is activated. A mantrap is a small room with two doors. The first door is locked; a person is identified and authenticated by a security guard, biometric system, smart card reader, or swipe card reader. Once the person is authenticated and access is authorized, the first door opens and allows the person into the mantrap. The first door locks and the person is trapped. The person must be authenticated again before the second door unlocks and allows him into the facility. Some mantraps use biometric systems that weigh the person who enters, to ensure only one person at a time is entering the mantrap area. This is a control to counter piggybacking.
Doorways with automatic locks can be configured to be fail-secure or fail-safe. A _fail-safe_ setting means that if a power disruption occurs that affects the automated locking system, the doors default to being unlocked. A _fail-secure_ configuration means that the doors default to being locked if there are any problems with the power.

**Windows**  Windows should be properly placed (this is where security and aesthetics can come to blows) and should have frames of the proper strengths, the necessary glazing material, and possibly have a protective covering. The glazing material, which is applied to the windows as they are being made, may be standard, tempered, acrylic, wire, or laminated on glass. _Standard glass_ windows are commonly used in residential homes and are easily broken. _Tempered glass_ is made by heating the glass and then suddenly cooling it. This increases its mechanical strength, which means it can handle more stress and is harder to break. It is usually five to seven times stronger than standard glass.

_Acrylic glass_ can be made out of polycarbonate acrylic, which is stronger than standard glass but produces toxic fumes if burned. Polycarbonate acrylics are stronger than regular acrylics, but both are made out of a type of transparent plastic. Because of their combustibility, their use may be prohibited by fire codes. The strongest window material is glass-clad polycarbonate. It is resistant to a wide range of threats (fire, chemical, breakage), but of course is much more expensive. These types of windows would be used in areas that are under the greatest threat.

Some windows are made out of glass that has _embedded wires_—in other words, it actually has two sheets of glass, with the wiring in between. The wires help reduce the likelihood of the window being broken or shattering.

_Laminated glass_ has two sheets of glass with a plastic film in between. This added plastic makes it much more difficult to break the window. As with other types of glass, laminated glass can come in different depths. The greater the depth (more glass and plastic), the more difficult it is to break.

A lot of window types have a film on them that provides efficiency in heating and cooling. They filter out UV rays and are usually tinted, which can make it harder for the bad guy to peep in and monitor internal activities. Some window types have a different kind of film applied that makes it more difficult to break them, whether by explosive, storm, or intruder.

**Internal Compartments**
Many components that make up a facility must be looked at from a security point of view. _Internal partitions_ are used to create barriers between one area and another. These partitions can be used to segment separate work areas, but should never be used in protected areas that house sensitive systems and devices. Many buildings have dropped ceilings, meaning the interior partitions do not extend to the true ceiling—only to the dropped ceiling. An intruder can lift a ceiling panel and climb over the partition. This example of intrusion is shown in Figure 6-4. In many situations, this would not require forced entry, specialized tools, or much effort. (In some office buildings, this may even be possible from a common public-access hallway.) These types of internal partitions should not be relied upon to provide protection for sensitive areas.
Computer and Equipment Rooms

It used to be necessary to have personnel within the computer rooms for proper maintenance and operations. Today, most servers, routers, switches, mainframes, and other equipment housed in computer rooms can be controlled remotely. This enables computers to live in rooms that have fewer people milling around and spilling coffee. Because the computer rooms no longer have personnel sitting and working in them for long periods, the rooms can be constructed in a manner that is efficient for equipment instead of people.

---

Window Types

A security professional may be involved with the planning phase of building a facility, and each of these items comes into play when constructing a secure building and environment. The following sums up the types of windows that can be used:

- **Standard**: No extra protection. The cheapest and lowest level of protection.
- **Tempered**: Glass is heated and then cooled suddenly to increase its integrity and strength.
- **Acrylic**: A type of plastic instead of glass. Polycarbonate acrylcs are stronger than regular acrylcs.
- **Wired**: A mesh of wire is embedded between two sheets of glass. This wire helps prevent the glass from shattering.
- **Laminated**: The plastic layer between two outer glass layers. The plastic layer helps increase its strength against breakage.
- **Solar window film**: Provides extra security by being tinted and offers extra strength due to the film’s material.
- **Security film**: Transparent film is applied to the glass to increase its strength.

---

**Figure 6-4** An intruder can lift ceiling panels and enter a secured area with little effort.
Smaller systems can be stacked vertically to save space. They should be mounted on racks or placed inside equipment cabinets. The wiring should be close to the equipment to save on cable costs and to reduce tripping hazards.

Data centers, server rooms, and wiring closets should be located in the core areas of a facility, near wiring distribution centers. Strict access control mechanisms and procedures should be implemented for these areas. The access control mechanisms may be smart card readers, biometric readers, or combination locks, as described in Chapter 4. These restricted areas should have only one access door, but fire code requirements typically dictate there must be at least two doors to most data centers and server rooms. Only one door should be used for daily entry and exit and the other door should be used only in emergency situations. This second door should not be an access door, which means people should not be able to come in through this door. It should be locked, but should have a panic bar that will release the lock if pressed.

These restricted areas ideally should not be directly accessible from public areas like stairways, corridors, loading docks, elevators, and restrooms. This helps ensure that the people who are by the doors to secured areas have a specific purpose for being there, versus being on their way to the restroom or standing around in a common area gossiping about the CEO.

Because data centers usually hold expensive equipment and the company’s critical data, their protection should be thoroughly thought out before implementation. Data centers should not be located on the top floors because it would be more difficult for an emergency crew to access it in a timely fashion in case of a fire. By the same token, data centers should not be located in basements where flooding can affect the systems. And if a facility is in a hilly area, the data center should be located well above ground level. Data centers should be located at the core of a building, to provide protection from natural disasters or bombs and to provide easier access to emergency crews if necessary.

Which access controls and security measures should be implemented for the data center depends upon the sensitivity of the data being processed and the protection level required. Alarms on the doors to the data processing center should be activated during off-hours and there should be policies dictate how to carry out access control during normal business hours, after hours, and during emergencies. If a combination lock is used to enter the data processing center, the combination should be changed at least every six months and also after an employee who knows the code leaves the company.

The various controls discussed next are shown in Figure 6-5. The team responsible for designing a new data center (or evaluating a current data center) should understand all the controls shown in Figure 6-5 and be able to choose what is needed.

The data processing center should be constructed as one room rather than different individual rooms. The room should be away from any of the building’s water pipes in case a break in a line causes a flood. The vents and ducts from the HVAC system should be protected with some type of barrier bars and should be too small for anyone to crawl through and gain access to the center. The data center must have positive air pressure, so no contaminants can be sucked into the room and into the computers’ fans.

In many data centers, an emergency Off switch is situated next to the door so someone can turn off the power if necessary. If a fire occurs, this emergency Off switch should be flipped as employees are leaving the room and before the fire suppression
agent is released. This is critical if the suppression agent is water, because water and electricity are not a good match—especially during a fire. A company can install a fire suppression system that is tied into this switch, so when a fire is detected, the electricity is automatically shut off right before the suppression material is released. (The suppression material could be a type of gas, such as halon, or FM-200, or water. Gases are usually a better choice for environments filled with computers. We will cover different suppression agents in the “Fire Prevention, Detection, and Suppression” section later in the chapter.)

Portable fire extinguishers should be located close to the equipment and should be easy to see and access. Smoke detectors or fire sensors should be implemented, and water sensors should be placed under the raised floors. Since most of the wiring and cables run under the raised floors, it is important that water does not get to these places and, if it does, that an alarm sound if water is detected.

**NOTE** If there is any type of water damage in a data center or facility, mold and mildew could easily become a problem. Instead of allowing things to “dry out on their own,” many times it is better to use industry-strength dehumidifiers, water movers, and sanitizers to ensure secondary damage does not occur.
Although water is very useful, sometimes it is not our best friend. Water can cause extensive damage to equipment, flooring, walls, computers, and facility foundations. It is important that an organization be able to detect leaks and unwanted water. The detectors should be under raised floors and on dropped ceilings (to detect leaks from the floor above it). The location of the detectors should be documented and their position marked for easy access. As smoke and fire detectors should be tied to an alarm system, so should water detectors. The alarms usually just alert the necessary staff members and not everyone in the building. The staff members who are responsible for following up when an alarm sounds should be trained properly on how to reduce any potential water damage. Before any poking around to see where water is or is not pooling in places it does not belong, the electricity for that particular zone of the building should be temporarily turned off.

Water detectors can help prevent damage to:

- Equipment
- Flooring
- Walls
- Computers
- Facility foundations

Location of water detectors should be:

- Under raised floors
- On dropped ceilings

It is important to maintain the proper temperature and humidity levels within data centers, which is why an HVAC system should be implemented specifically for this room. Too high of a temperature can cause components to overheat and turn off; too low of a temperature can cause the components to work more slowly. If the humidity is high, then corrosion of the computer parts can take place; if humidity is low, then static electricity can be introduced. Because of this, the data center must have its own temperature and humidity controls, which are separate from the rest of the building.

It is best if the data center is on a different electrical system than the rest of the building, if possible. Thus, if anything negatively affects the main building’s power, it will not carry over and affect the center. The data center may require redundant power supplies, which means two or more feeders coming in from two or more electrical substations. The idea is that if one of the power company’s substations were to go down, the company would still be able to receive electricity from the other feeder. But just because a company has two or more electrical feeders coming into its facility does not mean true redundancy is automatically in place. Many companies have paid for two feeders to come into their building, only to find out both feeders were coming from the same substation! This defeats the whole purpose of having two feeders in the first place.

Data centers need to have their own backup power supplies, either an uninterruptible power supply (UPS) or generators. The different types of backup power supplies are discussed later in the chapter, but it is important to know at this point that the power backup must be able to support the load of the data center.
Many companies choose to use large glass panes for the walls of the data center so personnel within the center can be viewed at all times. This glass should be shatter-resistant since the window is acting as an exterior wall. The center’s doors should not be hollow, but rather secure solid-core doors. Doors should open out rather than in so they don’t damage equipment when opened. Best practices indicate that the door frame should be fixed to adjoining wall studs and that there should be at least three hinges per door. These characteristics would make the doors much more difficult to break down.

**Protecting Assets**

The main threats that physical security components combat are theft, interruptions to services, physical damage, compromised system and environment integrity, and unauthorized access.

Real loss is determined by the cost to replace the stolen items, the negative effect on productivity, the negative effect on reputation and customer confidence, fees for consultants that may need to be brought in, and the cost to restore lost data and production levels. Many times, companies just perform an inventory of their hardware and provide value estimates that are plugged into risk analysis to determine what the cost to the company would be if the equipment were stolen or destroyed. However, the information held within the equipment may be much more valuable than the equipment itself, and proper recovery mechanisms and procedures also need to be plugged into the risk assessment for a more realistic and fair assessment of cost.

Laptop theft is increasing at incredible rates each year. They have been stolen for years, but in the past they were stolen mainly to sell the hardware. Now laptops are also being stolen to gain sensitive data for identity theft crimes. The CSI/FBI 2003 Computer Crime and Security Survey indicates that U.S. companies lost around $6.8 million in laptop theft. Gartner Group estimates that a stolen laptop costs a company around $6000, which does not account for any data lost or potential exposure to secondary crimes. *Time* magazine estimated that 1600 laptops are stolen each day in the U.S. alone. These thefts take place in airports, hotels, from cars, and within office buildings. In August 2002, close to 2000 Internal Revenue Service laptops that may have contained taxpayers’ confidential information went unaccounted for. In August 2002, five agencies under Justice Department jurisdiction reported 400 missing laptop computers. The classification level of 218 of the missing laptops was unknown, and the report noted, “It is possible that the missing laptop computers would have been used to process and store national security or sensitive law enforcement information that, if divulged, could harm the public.”

In June 2004, GMAC Financial Services had two laptops stolen from an employee’s car that exposed about 200,000 of its customers’ personal data. In May 2005, MCI had a laptop stolen that contained around 16,500 current and former employees’ personal information. This list could go on and on for hundreds of pages. What is important to understand is that this is a rampant, and potentially very dangerous, crime. Many people claim, “My whole life is on my laptop” or possibly their PDA. Since employees use laptops as they travel, they may have extremely sensitive company or customer data on their systems that can easily fall into the wrong hands. The following list provides many of the protection mechanisms that can be used to protect laptops and the data they hold:
• Inventory all laptops, including serial numbers so they can be properly identified if recovered.
• Harden the operating system.
• Password protect the BIOS.
• Register all laptops with the vendor and file a report when one is stolen. If a stolen laptop is sent in for repairs, it will be flagged by the vendor.
• Do not check a laptop as luggage when flying.
• Never leave a laptop unattended, and carry it in a nondescript carrying case.
• Engrave the laptop with a symbol or number for proper identification.
• Use a slot lock with a cable to connect a laptop to a stationary object.
• Back up the data from the laptop and store it on a stationary PC or backup media.
• Use specialized safes if storing laptops in vehicles.
• Encrypt all sensitive data.

Tracing software can be installed so that your laptop can "phone home" if it is taken from you. Several products offer this tracing capability. Once installed and configured, the software periodically sends in a signal to a tracking center. If you report that your laptop has been stolen, the vendor of this software will work with service providers and law enforcement to track down and return your laptop.

A company may have need for a safe. Safes are commonly used to store backup data tapes, original contracts, or other types of valuables. The safe should be penetration-resistant and provide fire protection. The types of safes an organization can choose from are:

- Wall safe  Embedded into the wall and easily hidden
- Floor safe  Embedded into the floor and easily hidden
- Chests  Stand-alone safes
- Depositories  Safes with slots, which allow the valuables to be easily slipped in
- Vaults  Safes that are large enough to provide walk-in access

If a safe has a combination lock, it should be changed periodically and only a small subset of people should have access to the combination or key. The safe should be in a visible location, so anyone who is interacting with the safe can be seen. The goal is to uncover any unauthorized access attempts. Some safes have passive or thermal relocking functionality. If the safe has a passive relocking function, it can detect when someone attempts to tamper with it, in which case extra internal bolts will fall into place to ensure it cannot be compromised. If a safe has a thermal relocking function, when a certain temperature is met (possibly from drilling), an extra lock is implemented to ensure the valuables are properly protected.
Internal Support Systems

This place has no air conditioning or water. Who would want to break into it anyway?

Having a fortified facility with secure compartmentalized areas and protected assets is nice, but having lights, air conditioning, and water within this facility is even better. Physical security needs to address these support services, because their malfunction or disruption could negatively affect the organization in many ways.

Although there are many incidents of various power losses here and there for different reasons (storms, hurricanes, California running out of electricity), one of the most notable power losses took place in August 2003 when eight East Coast states and portions of Canada lost power for several days. Although there were rumors about a worm causing this disruption, it was found to be a software bug in GE Energy’s XA/21 system. This disaster left over 50 million people without power for days, caused four nuclear power plants to be shut down, and put a lot of companies in insecure and chaotic states. Security professionals need to be able to help organizations handle both the small bumps in the road, such as power surges or sags, and the gigantic sinkholes, such as what happened in the United States and Canada on August 14, 2003.

Electric Power

We don’t need no stinkin’ power supply. Just rub these two sticks together.

Because computing and communication has become so essential in the corporate world, power failure is a much more devastating event than it was 10 to 15 years ago. The need for good plans to fall back on is crucial to provide the assurance that a business will not be drastically affected by storms, high winds, hardware failure, lightning, or other events that can stop or disrupt power supplies. A continuous supply of electricity assures the availability of company resources; thus, a security professional must be familiar with the threats to electric power and corresponding countermeasures.

Several types of power backup capabilities exist. Before a company chooses one, it should calculate the total cost of anticipated downtime and its effects. This information can be gathered from past records and other businesses in the same area on the same power grid. The total cost per hour for backup power is derived by dividing the annual expenditures by the annual standard hours of use.

Large and small issues can cause power failure or fluctuations. The effects manifest in variations of voltage that can last a millisecond to days. A company can pay to have two different supplies of power to reduce its risks, but this approach can be costly. Other, less expensive mechanisms are to have generators or UPSs in place. Some generators have sensors to detect power failure and will start automatically upon failure. Depending on the type and size of the generator, it might provide power for hours or days. UPSs are usually short-term solutions compared to generators.

Power Protection

Protecting power can be done in three ways: through UPSs, power line conditioners, and backup sources. UPSs use battery packs that range in size and capacity. A UPS can be online or standby. Online UPS systems use AC line voltage to charge a bank of bat-
teries. When in use, the UPS has an inverter that changes the DC output from the batteries into the required AC form and regulates the voltage as it powers computer devices. This conversion process is shown in Figure 6-6. Online UPS systems have the normal primary power passing through them day in and day out. They constantly provide power from their own inverters, even when the electric power is in proper use. Since the environment’s electricity passes through this type of UPS all the time, the UPS device is able to quickly detect when a power failure takes place. An online UPS can provide the necessary electricity and picks up the load after a power failure much more quickly than a standby UPS.

**Standby UPS** devices stay inactive until a power line fails. The system has sensors that detect a power failure, and the load is switched to the battery pack. The switch to the battery pack is what causes the small delay in electricity being provided. So an online UPS picks up the load much more quickly than a standby UPS, but costs more of course.

Backup power supplies are necessary when there is a power failure and the outage will last longer than a UPS can last. Backup supplies can be a redundant line from another electrical substation or from a motor generator, and can be used to supply main power or charge the batteries in a UPS system.

A company should identify critical systems that need protection from interrupted power supplies, and then estimate how long secondary power would be needed and how much power is required per device. Some UPS devices provide just enough power to allow systems to shut down gracefully, whereas others allow the systems to run for a longer period. A company needs to determine whether systems should only have a big enough power supply to allow them to shut down properly or whether they need a system that keeps them up and running so critical operations remain available.

Just having a generator in the closet should not give a company that warm fuzzy feeling of protection. An alternate power source should be tested periodically to make sure it works, and to the extent expected. It is never good to find yourself in an emergency only to discover the generator does not work, or someone forgot to buy the gas necessary to keep the thing running.

**Figure 6-6**  A UPS device converts DC current from its internal or external batteries to usable AC by using an inverter.
Electric Power Issues

Electric power enables us to be productive and functional in many different ways, but if it is not installed, monitored, and respected properly, it can do us great harm.

When clean power is being provided, the power supply contains no interference or voltage fluctuation. The possible types of interference (line noise) are electromagnetic interference (EMI) or radio frequency interference (RFI), which is disturbance to the flow of electric power while it travels across a power line, as shown in Figure 6-7. EMI can be created by the difference between three wires: hot, neutral, and ground, and the magnetic field they create. Lightning and electrical motors can induce EMI, which could then interrupt the proper flow of electrical current as it travels over wires to, from, and within buildings. RFI can be caused by anything that creates radio waves. Fluorescent lighting is one of the main causes of RFI within buildings today, so does that mean we need to rip out all the fluorescent lighting? Well, that is one choice, but we could also just use shielded cabling where fluorescent lighting could cause a problem. If you take a break from your reading, climb up into your office’s dropped ceiling, and look around, you would probably see wires bundled and tied up to the true ceiling. If your office is using fluorescent lighting, the power and data lines should not be running over, or on top of, the fluorescent lights. This is because the radio frequencies being given off can interfere with the data or power current as it travels through these wires. Now, get back down from the ceiling. We have work to do.

![Figure 6-7](image-url)  
**Figure 6-7**  RFI and EMI can cause line noise on power lines.
Interference interrupts the flow of an electrical current, and fluctuations can actually deliver a different level of voltage than what was expected. Each fluctuation can be damaging to devices and people. The following explains the different types of voltage fluctuations possible with electric power:

- **Power excess**
- **Spike**  Momentary high voltage
- **Surge**  Prolonged high voltage
- **Power loss**
- **Fault**  Momentary power outage
- **Blackout**  Prolonged, complete loss of electric power
- **Power degradation**
- **Sag/dip**  Momentary low voltage condition, from one cycle to a few seconds
- **Brownout**  Prolonged power supply that is below normal voltage
- **In-rush current**  Initial surge of current required to start a load

When an electrical device is turned on, it can draw a large amount of current, which is referred to as *in-rush current*. If the device sucks up enough current, it can cause a *sag* in the available power for surrounding devices. This could negatively affect their performance. As stated earlier, it is a good idea to have the data processing center and devices on a different electrical wiring segment from that of the rest of the facility, if possible, so the devices will not be affected by these issues. For example, if you are in a building or house without efficient wiring and you turn on a vacuum cleaner or microwave, you
may physically see the lights quickly dim because of this in-rush current. The drain on
the power supply caused by in-rush currents still happens in other environments when
these types of electrical devices are used—you just might not be able to physically see
the effects. Any type of device that would cause such a dramatic in-rush current should
not be used on the same electrical segment as data processing systems.

**Surge** A *surge* is a prolonged rise in voltage from a power source. Surges can cause
a lot of damage very quickly. A surge is one of the most common power problems and is
controlled with surge protectors. These protectors use a device called a *metal oxide varis-
tor*, which moves the excess voltage to ground when a surge occurs. Its source can be
from a strong lightning strike, a power plant going online or offline, a shift in the com-
mercial utility power grid, and electrical equipment within a business starting and stop-
ing. Most computers have a built-in surge protector in their power supplies, but these
are baby surge protectors and cannot provide protection against the damage that larger
surges (say, from storms) can cause. So, you need to ensure all devices are properly
plugged into larger surge protectors, whose only job is to absorb any extra current be-
fore it is passed to electrical devices.

**Blackout** A *blackout* is when the voltage drops to zero. This can be caused by light-
ing, a car taking out a power line, storms, or failure to pay the power bill. It can last for
seconds or days. This is when a backup power source is required for business continuity.

**Brownout** When power companies are experiencing high demand, they frequently
reduce the voltage in an electrical grid, which is referred to as a *brownout*. Constant-
voltage transformers can be used to regulate this fluctuation of power. They can use
different ranges of voltage and only release the expected 120 volts of alternating current
to devices.

**Noise** Noise on power lines can be a result of lightning, the use of fluorescent light-
ing, a transformer being hit by an automobile, or other environmental or human ac-
tivities. Frequency ranges overlap, which can affect electrical device operations. Light-
ning sometimes produces voltage spikes on communications and power lines, which
can destroy equipment or alter data being transmitted. When generators are switched
on because power loads have increased, they too can cause voltage spikes that can be
harmful and disruptive. Storms and intense cold or heat can put a heavier load on gen-
erators and cause a drop in voltage. Each of these instances is an example of how nor-
mal environmental behaviors can affect power voltage, eventually adversely affecting
equipment, communications, or the transmission of data.

Because these and other occurrences are common, mechanisms should be in place
to detect unwanted power fluctuations and protect the integrity of your data processing
environment. *Voltage regulators* and *line conditioners* can be used to ensure a clean and
smooth distribution of power. The primary power runs through a regulator or condi-
tioner. They have the capability to absorb extra current if there is a spike, and to store
energy to add current to the line if there is a sag. The goal is to keep the current flowing
at a nice, steady level so neither motherboard components nor employees get fried.
Many data centers are constructed to take power-sensitive equipment into consideration. Because surges, sags, brownouts, blackouts, and voltage spikes frequently cause data corruption, the centers are built to provide a high level of protection against these events. Other types of environments usually are not built with these things in mind and do not provide this level of protection. Offices usually have different types of devices connected and plugged into the same outlets. Outlet strips are plugged into outlet strips, which are connected to extension cords. This causes more line noise and a reduction of voltage to each device. Figure 6-8 depicts an environment that can cause line noise, voltage problems, and possibly a fire hazard.

**Preventive Measures and Good Practices**

*Don’t stand in a pool of water with a live electrical wire.*

*Response: Hold on, I need to write that one down.*

When dealing with electric power issues, the following items can help protect devices and the environment:

- Plug in every device to a surge protector to protect from excessive current.
- Shut down devices in an orderly fashion to help avoid data loss or damage to devices due to voltage changes.
- Employ power line monitors to detect frequency and voltage amplitude changes.

*Figure 6-8*  This configuration can cause a lot of line noise and poses a fire hazard.
Use regulators to keep voltage steady and the power clean.

Protect distribution panels, master circuit breakers, and transformer cables with access controls.

Provide protection from magnetic induction through shielded lines.

Use shielded cabling for long cable runs.

Do not run data or power lines directly over fluorescent lights.

Use three-prong connections or adapters if using two-prong cables.

Do not plug outlet strips and extension cords into each other.

Environmental Issues

Improper environmental controls can cause damage to services, hardware, and lives. Interruption of some services can cause unpredicted and unfortunate results. Power, heating, ventilation, air-conditioning, and air-quality controls can be complex and contain many variables. They all need to be operating properly and be monitored regularly.

During facility construction, the physical security team must make certain that water, steam, and gas lines have proper shutoff valves, as shown in Figure 6-9, and positive drains, which means their contents flow out instead of in. If there is ever a break in a main water pipe, the valve to shut off water flow must be readily accessible. Similarly, in case of fire in a building, the valve to shut off the gas lines must be readily accessible. In case of a flood, a company wants to ensure that material cannot travel up through the water pipes and into its water supply or facility. Facility, operations, and security personnel should know where these shutoff valves are, and there should be strict procedures to follow in these types of emergencies. This will help reduce the potential damage.

Figure 6-9
Water, steam, and gas lines should have emergency shutoff valves.
Most electronic equipment must operate in a climate-controlled atmosphere. Although it is important to keep the atmosphere at a proper working temperature, it is important to understand that the components within the equipment can suffer from overheating even in a climate-controlled atmosphere if the internal computer fans are not cleaned or are blocked. When devices are overheated, the components can expand and contract, which causes components to change their electronic characteristics, reducing their effectiveness or damaging the system overall.

**NOTE** The climate issues involved with a data processing environment are why it needs its own separate HVAC system. Maintenance procedures should be documented and properly followed. HVAC activities should be recorded and reviewed annually.

Maintaining appropriate temperature and humidity is important in any facility, especially facilities with computer systems. Improper levels of either can cause damage to computers and electrical devices. High humidity can cause corrosion, and low humidity can cause excessive static electricity. This static electricity can short out devices, cause the loss of information, or provide amusing entertainment for unsuspecting employees.

Lower temperatures can cause mechanisms to slow or stop, and higher temperatures can cause devices to use too much fan power and eventually shut down. Table 6-1 lists different components and their corresponding damaging temperature levels.

In drier climates, or during the winter, the air contains less moisture, which can cause static electricity when two dissimilar objects touch each other. This electricity usually travels through the body and produces a spark from a person’s finger that can release several thousand volts. This can be more damaging than you would think. Usually the charge is released on a system casing and is of no concern, but sometimes it is released directly to an internal computer component and causes damage. People who work on the internal parts of a computer usually wear antistatic armbands to reduce the chance of this happening.

In more humid climates, or during the summer, more humidity is in the air, which can also affect components. Particles of silver can begin to move away from connectors onto copper circuits, which cement the connectors into their sockets. This can adversely affect the electrical efficiency of the connection. A hygrometer is usually used to monitor humidity. It can be manually read, or an automatic alarm can be set up to go off if the humidity passes a set threshold.

### Preventive Steps Against Static Electricity

The following are some simple measures to prevent static electricity:

- Use antistatic flooring in data processing areas.
- Ensure proper humidity.
- Have proper grounding for wiring and outlets.
- Don’t have carpeting in data centers, or have static-free carpets if necessary.
- Wear antistatic bands when working inside computer systems.
Can I smoke in the server room?
Response: Security!

Air ventilation has several requirements that must be met to ensure a safe and comfortable environment. A closed-loop recirculating air-conditioning system should be installed to maintain air quality. “Closed-loop” means the air within the building is reused after it has been properly filtered, instead of bringing outside air in. Positive pressurization and ventilation should also be implemented to control contamination. Positive pressurization means that when an employee opens a door, the air goes out, and outside air does not come in. If a facility was on fire, you would want the smoke to go out the doors instead of being pushed back in when people are fleeing.

The assessment team needs to understand the various types of contaminants, how they can enter an environment, the damage they could cause, and the steps to ensure that a facility is protected from dangerous substances or high levels of average contaminants. Airborne material and particle concentrations must be monitored for inappropriate levels. Dust can affect a device’s functionality by clogging up the fan that is supposed to be cooling the device. Excessive concentrations of certain gases can accelerate corrosion and cause performance issues or failure of electronic devices. Although most disk drives are hermetically sealed, other storage devices can be affected by airborne contaminants. Air-quality devices and ventilation systems deal with these issues.

### Table 6-1

<table>
<thead>
<tr>
<th>Component Affected by Specific Temperatures</th>
<th>Material or Component</th>
<th>Damaging Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer systems and peripheral devices</td>
<td>175°F</td>
<td></td>
</tr>
<tr>
<td>Magnetic storage devices</td>
<td>100°F</td>
<td></td>
</tr>
<tr>
<td>Paper products</td>
<td>350°F</td>
<td></td>
</tr>
</tbody>
</table>

**Fire Prevention, Detection, and Suppression**

We can either try to prevent fires or have one really expensive weenie-roast.

The subject of physical security would not be complete without a discussion on fire safety. A company must meet national and local standards pertaining to fire prevention, detection, and suppression methods. Fire prevention includes training employees on how to react properly when faced with a fire, supplying the right equipment and ensuring it is in working order, making sure there is an easily reachable fire suppression supply, and storing combustible elements in the proper manner. Fire prevention may also include using proper noncombustible construction materials and designing the facility with containment measures that provide barriers to minimize the spread of fire and smoke. These thermal or fire barriers can be made up of different types of construction material that is noncombustible and has a fire-resistant coating applied to them.

Fire detection response systems come in many different forms. Manual detection response systems are the red pull boxes you see on many building walls. Automatic detection response systems have sensors that react when they detect the presence of fire or smoke. We will review different types of detection systems in the next section.
Fire suppression is the use of a suppression agent to put out a fire. Fire suppression can take place manually through handheld portable extinguishers, or automatically through automated systems such as water sprinkler systems, or halon or CO₂ discharge systems. The upcoming “Fire Suppression” section reviews the different types of suppression agents and where they are best used. Automatic sprinkler systems are widely used and highly effective in protecting buildings and their contents. When deciding upon the type of fire suppression systems to install, a company needs to evaluate many factors, including an estimate of the occurrence rate of a possible fire, the amount of damage that could result, the types of fires that would most likely take place, and the types of suppression systems to choose from.

Fire protection processes should consist of implementing early smoke or fire detection devices and shutting down systems until the source of the heat is eliminated. A warning signal may be sounded by a smoke or fire detector before the suppression agent is released, so that if it is a false alarm or a small fire that can be handled without the automated suppression system, someone has time to shut down the suppression system.

Types of Fire Detection
Fires present a dangerous security threat because they can damage hardware and data and risk human life. Smoke, high temperatures, and corrosive gases from a fire can cause devastating results. It is important to evaluate the fire safety measurements of a building and the different sections within it.

A fire begins because something ignited it. Ignition sources can be failure of an electrical device, improper storage of combustible materials, carelessly discarded cigarettes, malfunctioning heating devices, and arson. A fire needs fuel (paper, wood, liquid, and so on) and oxygen to continue to burn and grow. The more fuel per square meter, the more intense the fire will become. A facility should be built, maintained, and operated to minimize the accumulation of fuels that can feed fires.

Fire Resistant Ratings
Fire resistant ratings are the result of tests carried out in laboratories using specific configurations of environmental settings. The American Society for Testing and Materials (ASTM) is the organization that creates the standards that dictate how these tests should be performed and how to properly interpret the test results. ASTM accredited testing centers carry out the evaluations in accordance with these standards and assign fire resistant ratings that are then used in federal and state fire codes. The tests evaluate the fire resistance of different types of materials in various environmental configurations. Fire resistance represents the ability of a laboratory-constructed assembly to contain a fire for a specific period of time. For example, a 5/8-inch-thick drywall sheet installed on each side of a wood stud provides a one-hour rating. If the thickness of this drywall is doubled, then this would be given a two-hour rating. The rating system is used to classify different building components.
There are four classes (A, B, C, and D) of fire, which are explained in the “Fire Suppression” section. You need to know the differences between the types of fire so you know how to properly extinguish each type. Portable fire extinguishers have markings that indicate what type of fire they should be used on, as illustrated in Figure 6-10. The markings denote what types of chemicals are within the canisters and what types of fires they have been approved to be used on. Portable extinguishers should be located within 50 feet of any electrical equipment, and also near exits. The extinguishers should be marked clearly, with an unobstructed view. They should be easily reachable and operational by employees, and inspected quarterly.

A lot of computer systems are made of components that are not combustible but that will melt or char if overheated. Most computer circuits use only two to five volts of direct current, which usually cannot start a fire. If a fire does happen in a computer room, it will most likely be an electrical fire caused by overheating of wire insulation or by overheating components that ignite surrounding plastics. Prolonged smoke usually occurs before combustion.

Several types of detectors are available, each of which works in a different way. The detector can be activated by smoke or heat.

**Smoke Activated** Smoke-activated detectors are good for early-warning devices. They can be used to sound a warning alarm before the suppression system activates. A **photoelectric device**, also referred to as an optical detector, detects the variation in light intensity. The detector produces a beam of light across a protected area, and if the beam is obstructed, the alarm sounds. Figure 6-11 illustrates how a photoelectric device works.
Another type of photoelectric device samples the surrounding air by drawing air into a pipe. If the light source is obscured, the alarm will sound.

**Heat Activated**  Heat-activated detectors can be configured to sound an alarm either when a predefined temperature (fixed temperature) is reached or when the temperature increases over a period of time (rate-of-rise). *Rate-of-rise temperature sensors* usually provide a quicker warning than *fixed-temperature sensors* because they are more sensitive, but they can also cause more false alarms. The sensors can either be spaced uniformly throughout a facility, or implemented in a line type of installation, which is operated by a heat-sensitive cable.

It is not enough to have these fire and smoke detectors installed in a facility; they must be installed in the right places. Detectors should be installed both on and above suspended ceilings and below raised floors, because companies run many types of wires in both places that could start an electrical fire. No one would know about the fire until it broke through the floor or dropped ceiling if detectors were not placed in these areas. Detectors should also be located in enclosures and air ducts, because smoke can gather in these areas before entering other spaces. It is important that people are alerted about a fire as quickly as possible so damage may be reduced, fire suppression activities may start quickly, and lives may be saved. Figure 6-12 illustrates the proper placement of smoke detectors.

**Automatic Dial-Up Alarm**

Fire detection systems can be configured to call the local fire station, and possibly the police station, to report a detected fire. The system plays a prerecorded message that gives the necessary information so officials can properly prepare for the stated emergency and arrive at the right location.
Fire Suppression

*How about if I just spit on the fire?*

*Response: I’m sure that will work just fine.*

It is important to know the different types of fires and what should be done to properly suppress them. Each fire type has a rating that indicates what materials are burning. Table 6-2 shows the four types of fire and their suppression methods, which all employees should know.

### Plenum Area

Wiring and cables are strung through *plenum areas*, such as the space above dropped ceilings, the space in wall cavities, and the space under raised floors. Plenum areas should have fire detectors. Also, only plenum-rated cabling should be used in plenum areas, which is cabling that is made out of material that does not let off hazardous gases if it burns.
You can suppress a fire in several ways, all of which require that certain precautions be taken. In many buildings, suppression agents located in different areas are designed to initiate after a specific trigger has been set off. Each agent has a zone of coverage, meaning an area that the agent supplier is responsible for. If a fire ignites within a certain zone, it is the responsibility of that suppression agent device to initiate, and then suppress that fire. Different types of suppression agents available include water, halon, foams, CO₂, and more. CO₂ is good for putting out fires but bad for many types of life forms. If an organization uses CO₂, the suppression releasing device should have a delay mechanism within it that makes sure the agent does not start applying CO₂ to the area until after an audible alarm has sounded and people have been given time to evacuate. CO₂ is a colorless, odorless substance that is potentially lethal because it removes oxygen from the air. Gas masks do not provide protection against CO₂. This type of fire suppression mechanism is best used in unattended facilities and areas.

For Class B and C fires, specific types of dry powders can be used, which include sodium or potassium bicarbonate, calcium carbonate, or monoammonium phosphate. The first three powders interrupt the chemical combustion of a fire. Monoammonium phosphate melts at low temperatures and excludes oxygen from the fuel.

Foams are mainly water-based and contain a foaming agent that allows them to float on top of a burning substance to exclude the oxygen.

### Table 6-2  Four Types of Fire and Their Suppression Methods

<table>
<thead>
<tr>
<th>Fire Class</th>
<th>Type of Fire</th>
<th>Elements of Fire</th>
<th>Suppression Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Common combustibles</td>
<td>Wood products, paper, and laminates</td>
<td>Water, foam</td>
</tr>
<tr>
<td>B</td>
<td>Liquid</td>
<td>Petroleum products and coolants</td>
<td>Gas, CO₂, foam, dry powders</td>
</tr>
<tr>
<td>C</td>
<td>Electrical</td>
<td>Electrical equipment and wires</td>
<td>Gas, CO₂, dry powders</td>
</tr>
<tr>
<td>D</td>
<td>Combustible metals</td>
<td>Magnesium, sodium, potassium</td>
<td>Dry powder</td>
</tr>
</tbody>
</table>

**Halon**

Halon is a gas that was widely used in the past to suppress fires because it interferes with the chemical combustion of the elements within a fire. It mixes quickly with the air and does not cause harm to computer systems and other data processing devices. It was used mainly in data centers and server rooms.

It was discovered that halon has chemicals (chlorofluorocarbons) that deplete the ozone and that concentrations greater than 10 percent are dangerous to people. Halon used on extremely hot fires degrades into toxic chemicals, which is even more dangerous to humans.
Some really smart people figured that the ozone was important to keep around, which caused halon to be federally restricted, and no companies are allowed to purchase and install new halon extinguishers. Companies that still have halon systems have been instructed to replace them with nontoxic extinguishers. The following are EPA-approved replacements for halon:

- FM-200
- NAF-S-III
- CEA-410
- FE-13
- Water
- Inergen
- Argon
- Argonite

NOTE There is actually a Class K fire, for commercial kitchens. These fires should be put out with a wet chemical, which is usually a solution of potassium acetate. This chemical works best when putting out cooking oil fires.

A fire needs fuel, oxygen, and high temperatures. Table 6-3 shows how different suppression substances interfere with these elements of fire.

By law, companies that have halon extinguishers do not have to replace them, but the extinguishers cannot be refilled. So, companies that have halon extinguishers do not have to replace them right away, but when the extinguisher's lifetime runs out, FM-200 extinguishers or other EPA-approved chemicals should be used.

NOTE Halon has not been manufactured since January 1, 1992, by international agreement. The Montreal Protocol banned halon in 1987, and countries were given until 1992 to comply with these directives. The most effective replacement for halon is FM-200, which is similar to halon but does not damage the ozone.

<table>
<thead>
<tr>
<th>Combustion Elements</th>
<th>Suppression Methods</th>
<th>How Suppression Works</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuel</td>
<td>Soda acid</td>
<td>Removes fuel</td>
</tr>
<tr>
<td>Oxygen</td>
<td>Carbon dioxide</td>
<td>Removes oxygen</td>
</tr>
<tr>
<td>Temperature</td>
<td>Water</td>
<td>Reduces temperature</td>
</tr>
<tr>
<td>Chemical combustion</td>
<td>Gas—halon or halon substitute</td>
<td>Interferes with the chemical reactions between elements</td>
</tr>
</tbody>
</table>

Table 6-3 How Different Substances Interfere with Elements of Fire
The HVAC system should be connected to the fire alarm and suppression system so it properly shuts down if a fire is identified. A fire needs oxygen, and this type of system can feed oxygen to the fire. Plus, the HVAC can spread deadly smoke into all areas of the building. Many fire systems can configure the HVAC to shut down if a fire alarm is triggered.

**Water Sprinklers**

I’m hot. Go pull that red thingy on the wall. I need some water.

Water sprinklers typically are simpler and less expensive than halon and FM-200 systems but can cause water damage. In an electrical fire, the water can increase the intensity of the fire, because it can work as a conductor for electricity—only making the situation worse. If water is going to be used in any type of environment with electrical equipment, the electricity must be turned off before the water is released. Sensors should be used to shut down the electric power before water sprinklers activate. Each sprinkler head should activate individually to avoid wide-area damage, and there should be shutoff valves so the water supply can be stopped if necessary.

A company should take great care in deciding which suppression agent and system is best for it. Four main types of water sprinkler systems are available: wet pipe, dry pipe, preaction, and deluge.

- **Wet pipe**  
  Wet pipe systems always contain water in the pipes and are usually discharged by temperature control level sensors. One disadvantage of wet pipe systems is that the water in the pipes may freeze in colder climates. Also, if there is a nozzle or pipe break, it can cause extensive water damage. These types of systems are also called closed head systems.

- **Dry pipe**  
  In dry pipe systems, the water is not actually held in the pipes. The water is contained in a “holding tank” until it is released. The pipes hold pressurized air, which is reduced when a fire or smoke alarm is activated, allowing the water valve to be opened by the water pressure.

  Water is not allowed into the pipes that feed the sprinklers until an actual fire is detected. First, a heat or smoke sensor is activated; then, the water fills the pipes leading to the sprinkler heads, the fire alarm sounds, the electric power supply is disconnected, and finally water is allowed to flow from the sprinklers. These pipes are best used in colder climates because the pipes will not freeze. Figure 6-13 depicts a dry pipe system.

- **Preaction**  
  Preaction systems are similar to dry pipe systems in that the water is not held in the pipes but is released when the pressurized air within the pipes is reduced. Once this happens, the pipes are filled with water, but it is not released right away. A thermal-fusible link on the sprinkler head has to melt before the water is released. The purpose of combining these two techniques is to give people more time to respond to false alarms or to small fires that can be handled by other means. Putting out a small fire with
a handheld extinguisher is better than losing a lot of electrical equipment to water damage. These systems are usually used only in data processing environments rather than the whole building, because of the higher cost of these types of systems.

- **Deluge**  
  A **deluge system** has its sprinkler heads wide open to allow a larger volume of water to be released in a shorter period. Because the water being released is in such large volumes, these systems are usually not used in data processing environments.

### Perimeter Security

*Halt! Who goes there?*

The first line of defense is perimeter control at the site location, to prevent unauthorized access to the facility. As mentioned earlier in this chapter, physical security should be implemented by using a layered defense approach. For example, before an intruder can get to the written recipe for your company’s secret barbecue sauce, she will need to climb or cut a fence, slip by a security guard, pick a door lock, circumvent a biometric access control reader that protects access to an internal room, and then break into the safe that holds the recipe. The idea is that if an attacker breaks through one control layer, there will be others in her way before she can obtain the company’s crown jewels.

**NOTE**  
It is also important to have a diversity of controls. For example, if one key works on four different door locks, the intruder has to obtain only one key. Each entry should have its own individual key or authentication combination.
This defense model should work in two main modes: one mode during normal facility operations and another mode during the time the facility is closed. When the facility is closed, all doors should be locked with monitoring mechanisms in strategic positions to alert security personnel of suspicious activity. When the facility is in operation, security gets more complicated because authorized individuals need to be distinguished from unauthorized individuals. Perimeter security deals with facility and personnel access controls, external boundary protection mechanisms, intrusion detection, and corrective actions. The following sections describe the elements that make up these categories.

**Facility Access Control**

Access control needs to be enforced through physical and technical components when it comes to physical security. Physical access controls use mechanisms to identify individuals who are attempting to enter a facility or area. They make sure the right in-
individuals get in and the wrong individuals stay out, and provide an audit trail of these actions. Having personnel within sensitive areas is one of the best security controls because they can personally detect suspicious behavior. However, they need to be trained on what activity is considered suspicious and how to report such activity.

Before a company can put into place the proper protection mechanisms, it needs to conduct a detailed review to identify which individuals should be allowed into what areas. Access control points can be identified and classified as external, main, and secondary entrances. Personnel should enter and exit through a specific entry, deliveries should be made to a different entry, and sensitive areas should be restricted. Figure 6-14 illustrates the different types of access control points into a facility. After a company has identified and classified the access control points, the next step is to determine how to protect them.

**Locks**

Locks are inexpensive access control mechanisms that are widely accepted and used. They are considered delaying devices to intruders. The longer it takes to break or pick a lock, the longer a security guard or police officer has to arrive on the scene if the intruder has been detected. Almost any type of a door can be equipped with a lock, but keys can be easily lost and duplicated, and locks can be picked or broken. If a company depends solely on a lock-and-key mechanism for protection, an individual who has the key can come and go as he likes without control and can remove items from the premises without detection. Locks should be used as part of the protection scheme, but should not be the sole protection scheme.

Locks vary in functionality. Padlocks can be used on chained fences, preset locks are usually used on doors, and programmable locks (requiring a combination to unlock) are used on doors or vaults. Locks come in all types and sizes. It is important to have the right type of lock so it provides the correct level of protection.

**Figure 6-14**

Access control points should be identified, marked, and monitored properly.
To the curious mind or a determined thief, a lock is considered a little puzzle to solve, not a deterrent. In other words, locks may be merely a challenge, not necessarily something to stand in the way of malicious activities. Thus, you need to make the challenge difficult, through the complexity, strength, and quality of the locking mechanisms.

**NOTE**  The delay time provided by the lock should match the penetration resistance of the surrounding components (door, door frame, hinges). A smart thief takes the path of least resistance, which may be to pick the lock, remove the pins from the hinges, or just kick down the door.

**Mechanical Locks**  Two main types of mechanical locks are available: the warded lock and the tumbler lock. The *warded lock* is the basic padlock, as shown in Figure 6-15. It has a spring-loaded bolt with a notch cut in it. The key fits into this notch and slides the bolt from the locked to the unlocked position. The lock has *wards* in it, which are metal projections around the keyhole, as shown in Figure 6-16. The correct key for a specific warded lock has notches in it that fit in these projections and a notch to slide the bolt back and forth. These are the cheapest locks, because of their lack of any real sophistication, and are also the easiest to pick.

The *tumbler lock* has more pieces and parts than a ward lock. As shown in Figure 6-17, the key fits into a cylinder, which raises the lock metal pieces to the correct height so the bolt can slide to the locked or unlocked position. Once all of the metal pieces are at the correct level, the internal bolt can be turned. The proper key has the required size and sequences of notches to move these metal pieces into their correct position.

The three types of tumbler locks are the pin tumbler, wafer tumbler, and lever tumbler. The *pin tumbler* lock, shown in Figure 6-17, is the most commonly used tumbler lock. The key has to have just the right grooves to put all the spring-loaded pins in the right position so the lock can be locked or unlocked.
Wafer tumbler locks (also called disc tumbler locks) are the small, round locks you usually see on file cabinets. They use flat discs (wafers) instead of pins inside the locks. They often are used as car and desk locks. This type of lock does not provide much protection because it can be easily circumvented.

**NOTE** Some locks have interchangeable cores, which allow for the core of the lock to be taken out. You would use this type of lock if you wanted one key to open several locks. You would just replace all locks with the same core.
Combination locks, of course, require the correct combination of numbers to unlock them. These locks have internal wheels that have to line up properly before being unlocked. A user spins the lock interface left and right by so many clicks, which lines up the internal wheels. Once the correct turns have taken place, all the wheels are in the right position for the lock to release and open the door. The more wheels within the locks, the more protection provided. Electronic combination locks do not use internal wheels, but rather have a keypad that allows a person to type in the combination instead of turning a knob with a combination faceplate. An example of an electronic combination lock is shown in Figure 6-18.

Cipher locks, also known as programmable locks, are keyless and use keypads to control access into an area or facility. The lock requires a specific combination to be entered into the keypad and possibly a swipe card. They cost more than traditional locks, but their combinations can be changed, specific combination sequence values can be locked out, and personnel who are in trouble or under duress can enter a specific code that will open the door and initiate a remote alarm at the same time. Thus, compared to traditional locks, cipher locks can provide a much higher level of security and control over who can access a facility.

The following are some functionalities commonly available on many cipher combination locks that improve the performance of access control and provide for increased security levels:

- **Door delay**  If a door is held open for a given time, an alarm will trigger to alert personnel of suspicious activity.

- **Key override**  A specific combination can be programmed to be used in emergency situations to override normal procedures or for supervisory overrides.

- **Master keying**  Enables supervisory personnel to change access codes and other features of the cipher lock.

- **Hostage alarm**  If an individual is under duress and/or held hostage, a combination he enters can communicate this situation to the guard station and/or police station.

If a door is accompanied by a cipher lock, it should have a corresponding visibility shield so a bystander cannot see the combination as it is keyed in. Automated cipher locks must have a backup battery system and be set to unlock during a power failure so personnel are not trapped inside during an emergency.
NOTE It is important to change the combination of locks and use random combination sequences. Often, people do not change their combinations or clean the keypads, which allows an intruder to know what key values are used in the combination, because they are the dirty and worn keys. The intruder then just needs to figure out the right combination of these values.

Some cipher locks require all users to know and use the exact same combination, which does not allow for any individual accountability. Some of the more sophisticated cipher locks permit specific codes to be assigned to unique individuals. This provides more accountability, because each individual is responsible for keeping his access code secret, and entry and exit activities can be logged and tracked. These are usually referred to as smart locks, because they are designed to only allow authorized individuals access at certain doors at certain times.

NOTE Hotel key cards are also known as smart cards. They are programmed by the nice hotel guy or gal behind the counter. The access code on the card can allow access to a hotel room, workout area, business area, and better yet—the mini bar.

Device Locks Unfortunately, hardware has a tendency to “walk away” from facilities; thus, device locks are necessary to thwart these attempts. Cable locks consist of a vinyl-coated steel cable that can secure a computer or peripheral to a desk or other stationary components, as shown in Figure 6-19.

The following are some of the device locks available and their capabilities:

- **Switch controls** Cover on/off power switches.
- **Slot locks** Secure the system to a stationary component by the use of steel cable that is connected to a bracket mounted in a spare expansion slot.
- **Port controls** Block access to disk drives or unused serial or parallel ports.
- **Peripheral switch controls** Secure a keyboard by inserting an on/off switch between the system unit and the keyboard input slot.
- **Cable traps** Prevent the removal of input/output devices by passing their cables through a lockable unit.

**Figure 6-19**

FMJ/PADLOCK’s notebook security cable kit secures a notebook by enabling the user to attach the device to a stationary component within an area.
Administrative Responsibilities  It is important for a company to not only choose the right type of lock for the right purpose, but also to follow proper maintenance and procedures. Keys should be assigned by facility management, and this assignment should be documented. Procedures should be written out detailing how keys are to be assigned, inventoried, and destroyed when necessary, and what should happen if and when keys are lost. Someone on the company's facility management team should be assigned the responsibility of overseeing key and combination maintenance.

Most organizations have master keys and submaster keys for the facility management staff. A master key opens all the locks within the facility, and the submaster keys open one or more locks. Each lock has its own individual unique keys as well. So if a facility has 100 offices, the occupant of each office can have his or her own key. A master key allows access to all offices for security personnel and for emergencies. If one security guard is responsible for monitoring half the facility, the guard can be assigned one of the submaster keys for just those offices.

Since these master and submaster keys are powerful, they must be properly guarded and not widely shared. A security policy should outline what portions of the facility and which device types need to be locked. As a security professional, you should understand what type of lock is most appropriate for each situation, the level of protection provided by various types of locks, and how these locks can be circumvented.

Circumventing Locks  Each lock type has corresponding tools that can be used to pick it (open it without the key). A tension wrench is a tool shaped like an L and is used to apply tension to the internal cylinder of a lock. The lock picker uses a lock pick to manipulate the individual pins to their proper placement. Once certain pins are “picked” (put in their correct place), the tension wrench holds these down while the lock picker figures out the correct settings for the other pins. After the intruder determines the proper pin placement, the wrench is used to then open the lock.

Lock Strengths

Basically, three grades of locks are available:

- **Grade 1**  Commercial and industrial use
- **Grade 2**  Heavy-duty residential / light-duty commercial
- **Grade 3**  Residential/consumer expendable (that is, “throw-away” locks)

The cylinders within the locks fall into three main categories:

- **Low security**  No pick or drill resistance provided (can fall within any of the three grades of locks)
- **Medium security**  A degree of pick resistance protection provided (uses tighter and more complex keyways [notch combination]; can fall within any of the three grades of locks)
- **High security**  Pick resistance protection through many different mechanisms (only used in grade 1 and 2 locks)
Intruders may carry out another technique, referred to as **raking**. To circumvent a pin tumbler lock, a lock pick is pushed to the back of the lock and quickly slid out while providing upward pressure. This movement makes many of the pins fall into place. A tension wrench is also put in to hold the pins that pop into the right place. If all the pins do not slide to the necessary height for the lock to open, the intruder holds the tension wrench and uses a thinner pick to move the rest of the pins into place.

Now, if this is all too much trouble for the intruder, she can just drill the lock, use bolt cutters, or attempt to break through the door or the door frame, or remove the hinges. There are just so many choices for the bad guys.

**Personnel Access Controls**

Proper identification needs to verify whether the person attempting to access a facility or area should actually be allowed in. Identification and authentication can be verified by matching an anatomical attribute (biometric system), using smart or memory cards (swipe cards), presenting a photo ID to a security guard, using a key, or providing a card and entering a password or PIN.
A common problem with controlling authorized access into a facility or area is called piggybacking. This occurs when an individual gains unauthorized access by using someone else’s legitimate credentials or access rights. Usually an individual just follows another person closely through a door without providing any credentials. The best preventive measures against piggybacking are to have security guards at access points and to educate employees about good security practices.

If a company wants to use a card badge reader, it has several types of systems to choose from. Individuals usually have cards that have embedded magnetic strips that contain access information. The reader can just look for simple access information within the magnetic strip, or it can be connected to a more sophisticated system that scans the information, makes more complex access decisions, and logs badge IDs and access times.

If the card is a memory card, then the reader just pulls information from it and makes an access decision. If the card is a smart card, the individual may be required to enter a PIN or password, which the reader compares against the information held within the card or in an authentication server. (Memory and smart cards are covered in Chapter 4.)

These access cards can be used with user-activated readers, which just means the user actually has to do something—swipe the card or enter a PIN. System sensing access control readers, also called proximity devices or transponders, recognize the presence of an approaching object within a specific area. This type of system does not require the user to swipe the card through the reader. The reader sends out interrogating signals and obtains the access code from the card without the user having to do anything.

**NOTE**  
Electronic access control (EAC) tokens is a generic term used to describe proximity authentication devices, such as proximity readers, programmable locks, or biometric systems, which identify and authenticate users before allowing them entrance into physically controlled areas.

**External Boundary Protection Mechanisms**

Let’s build a fort and let only the people who know the secret handshake inside!

Proximity protection components are usually put into place to provide one or more of the following services:

- Control pedestrian and vehicle traffic flows
- Various levels of protection for different security zones
- Buffers and delaying mechanisms to protect against forced entry attempts
- Limit and control entry points

These services can be provided by using the following control types:

- **Access control mechanisms**  
  Locks and keys, an electronic card access system, personnel awareness

- **Physical barriers**  
  Fences, gates, walls, doors, windows, protected vents, vehicular barriers
Intrusion detection  Perimeter sensors, interior sensors, annunciation mechanisms

Assessment  Guards, CCTV cameras

Response  Guards, local law enforcement agencies

Deterrents  Signs, lighting, environmental design

Several types of perimeter protection mechanisms and controls can be put into place to protect a company's facility, assets, and personnel. They can deter would-be intruders, detect intruders and unusual activities, and provide ways of dealing with these issues when they arise. Perimeter security controls can be natural (hills, rivers) or manmade (fencing, lighting, gates). Landscaping is a mix of the two. In the beginning of this chapter, we explored CPTED and how this approach is used to reduce the likelihood of crime. Landscaping is a tool employed in the CPTED method. Sidewalks, bushes, and created paths can point people to the correct entry points, and trees and spiky bushes can be used as natural barriers. These bushes and trees should be placed such that they cannot be used as ladders or accessories to gain unauthorized access to unapproved entry points. Also, there should not be an overwhelming number of trees and bushes, which could provide intruders with places to hide. In the following sections, we look at the manmade components that can work within the landscaping design.

Fencing

I just want a little fence to keep out all the little mean people.

Fencing can be quite an effective physical barrier. Although the presence of a fence may only delay dedicated intruders in their access attempts, it can work as a psychological deterrent by telling the world that your company is serious about protecting itself.

Fencing can provide crowd control and helps control access to entrances and facilities. However, fencing can be costly and unsightly. Many companies plant bushes or trees in front of the fence that surrounds their buildings for aesthetics and to make the building less noticeable. But this type of vegetation can damage the fencing over time or negatively affect its integrity. The fencing needs to be properly maintained, because if a company has a sagging, rusted, pathetic fence, it is equivalent to telling the world that the company is not truly serious and disciplined about protection. But a nice, shiny, intimidating fence can send a different message—especially if the fencing is topped with three rungs of barbed wire.

When deciding upon the type of fencing, several factors should be considered. The gauge of the metal should correlate to the types of physical threats the company would most likely face. After carrying out the risk analysis (covered earlier in the chapter), the physical security team should understand the probability of enemies attempting to cut the fencing, drive through it, or climb over or crawl under it. Understanding these threats will help the team determine the necessary gauge and mesh sizing of the fence wiring.

The risk analysis results will also help indicate what height of fencing the organization should implement. Fences come in varying heights, and each height provides a different level of security:
• Fences three to four feet high only deter casual trespassers.
• Fences six to seven feet high are considered too high to climb easily.
• Fences eight feet high (possibly with strands of barbed or razor wire at the top) means you are serious about protecting your property. They often deter the more determined intruder.

The barbed wire on top of fences can be tilted in or out, which also provides extra protection. If the organization is a prison, it would have the barbed wire on top of the fencing pointed in, which makes it harder for prisoners to climb and escape. If the organization is a military base, the barbed wire would be tilted out, making it harder for someone to climb over the fence and gain access to the premises.

Critical areas should have fences at least eight feet high to provide the proper level of protection. The fencing should not sag in any areas and must be taut and securely connected to the posts. The fencing should not be easily circumvented by pulling up its posts. The posts should be buried sufficiently deep in the ground and should be secured with concrete to ensure the posts cannot be dug up or tied to vehicles and extracted. If the ground is soft or uneven, this might provide ways for intruders to slip or dig under the fence. In these situations, the fencing should actually extend into the dirt to thwart these types of attacks.

Fences work as “first line of defense” mechanisms. A few other controls can be used also. Strong and secure gates need to be implemented. It does no good to install a highly fortified and expensive fence and then have an unlocked or weenie gate that allows easy access.

### Gauges and Mesh Sizes

The gauge of fence wiring is the thickness of the wires used within the fence mesh. The lower the gauge number, the larger the wire diameter:

- **11 gauge** = 0.0907-inch diameter
- **9 gauge** = 0.1144-inch diameter
- **6 gauge** = 0.162-inch diameter

The mesh sizing is the minimum clear distance between the wires. Common mesh sizes are 2 inches, 1 inch, and 3/8 inch. It is more difficult to climb or cut fencing with smaller mesh sizes, and the heavier gauged wiring is harder to cut. The following list indicates the strength levels of the most common gauge and mesh sizes used in chain-link fencing today:

- **Extremely high security**  3/8-inch mesh, 11 gauge
- **Very high security**     1-inch mesh, 9 gauge
- **High security**          1-inch mesh, 11 gauge
- **Greater security**       2-inch mesh, 6 gauge
- **Normal industrial security**  2-inch mesh, 9 gauge
Chapters

Gates basically have four distinct classifications:

- **Class I** Residential usage.
- **Class II** Commercial usage, where general public access is expected; examples include a public parking lot entrance, a gated community, or a self storage facility.
- **Class III** Industrial usage, where limited access is expected; an example is a warehouse property entrance not intended to serve the general public.
- **Class IV** Restricted access; this includes a prison entrance that is monitored either in person or via closed circuitry.

Each gate classification has its own long list of implementation and maintenance guidelines in order to ensure the necessary level of protection. These classifications and guidelines are developed by Underwriters Laboratory (UL), a nonprofit organization that tests, inspects, and classifies electronic devices, fire protection equipment, and specific construction materials. This is the group that certifies these different items to ensure they are in compliance with national building codes. Their specific code, UL-325, deals with garage doors, drapery, gates, and louver and window operators and systems.

So, whereas in the information security world we look to NIST for our best practices and industry standards, in the physical security world, we look to UL for the same type of direction.

**NOTE**

UL standards can be found at [www.ul.com](http://www.ul.com). A good introduction to the UL-325 standard, which deals with gates, can be found at [www.abrpaint.com/services/GatesFencing/ul325intro.htm](http://www.abrpaint.com/services/GatesFencing/ul325intro.htm).

**Bollards**

*Bollards* usually look like small concrete pillars outside a building. Sometimes companies try to dress them up by putting flowers or lights in them to soften the look of a protected environment. They are placed by the sides of buildings that have the most immediate threat of someone driving a vehicle through the exterior wall. They are usually placed between the facility and a parking lot and/or between the facility and a road that runs close to an exterior wall. Within the United States after September 11, 2001, many military and government institutions, which did not have bollards, hauled in huge boulders to surround and protect sensitive buildings. They provided the same type of protection that bollards would provide. These were not overly attractive but provided the sense that the government was serious about protecting those facilities.
Lighting

Many of the items mentioned in this chapter are things people take for granted day in and day out during our usual busy lives. Lighting is certainly one of those items you would probably not give much thought to, unless it wasn’t there. Unlit (or improperly lit) parking lots and parking garages have invited many attackers to carry out criminal activity that they may not have engaged in otherwise if the proper lighting was in place. Breaking into cars, stealing cars, and attacking employees as they leave the office are the more common types of attacks that take place in such situations. A security professional should understand that the right illumination needs to be in place, that no dead spots (unlit areas) should exist between the lights, and that all areas where individuals may walk should be properly lit. A security professional should also understand the various types of lighting available and where they should be used.

Wherever an array of lights is used, each light covers its own zone or area. The zone each light covers depends upon the illumination of light produced, which usually has a direct relationship to the wattage capacity of the bulbs. In most cases, the higher the lamp’s wattage, the more illumination it produces. It is important that the zones of illumination coverage overlap. For example, if a company has an open parking lot, then light poles must be positioned within the correct distance of each other to eliminate any dead spots. If the lamps that will be used provide a 30-foot radius of illumination, then the light poles should be erected less than 30 feet apart so there is an overlap between the areas of illumination.

If an organization does not implement the right types of lights and ensure they provide proper coverage, it increases the probability of criminal activity, accidents, and lawsuits.

Exterior lights that provide protection usually require less illumination intensity than interior working lighting, except for areas that require security personnel to inspect identification credentials for authorization. It is also important to have the correct lighting when using various types of surveillance equipment. The correct contrast between a potential intruder and background items needs to be provided, which only happens with the correct illumination and placement of lights. If the light is going to bounce off of dark, dirty, or darkly painted surfaces, then more illumination is required for the necessary contrast between people and the environment. If the area has clean concrete and light-colored painted surfaces, then not as much illumination is required. This is because when the same amount of light falls on an object and the surrounding background, an observer must depend on the contrast to tell them apart.

When lighting is installed, it should be directed toward areas where potential intruders would most likely be coming from and directed away from the security force posts. For example, lighting should be pointed at gates or exterior access points, and the guard locations should be more in the shadows, or under a lower amount of illumination. This is referred to as glare protection for the security force. If you are familiar with military operations, you might know that when you are approaching a military entry point, there is a fortified guard building with lights pointing toward the oncoming cars. A large sign instructs you to turn off your headlights, so the guards are not temporarily blinded by your lights and have a clear view of anything coming their way.
Lights used within the organization’s security perimeter should be directed outward, which keeps the security personnel in relative darkness and allows them to easily view intruders beyond the company’s perimeter.

An array of lights that provides an even amount of illumination across an area is usually referred to as **continuous lighting**. Examples are the evenly spaced light poles in a parking lot, light fixtures that run across the outside of a building, or series of fluorescent lights used in parking garages. If the company building is relatively close to another company’s property, a railway, an airport, or a highway, the owner may need to ensure the lighting does not “bleed over” property lines in an obtrusive manner. Thus, the illumination needs to be **controlled**, which just means an organization should erect lights and use illumination in such a way that does not blind its neighbors or any passing cars, trains, or planes.

You probably are familiar with the special home lighting gadgets that turn certain lights on and off at predetermined times, giving the illusion to potential burglars that a house is occupied even when the residents are away. Companies can use a similar technology, which is referred to as **standby lighting**. The security personnel can configure the times that different lights turn on and off, so potential intruders think different areas of the facility are populated.

**NOTE** Redundant or backup lights should be available in case of power failures or emergencies. Special care must be given to understand what type of lighting is needed in different parts of the facility in these types of situations. This lighting may run on generators or battery packs.

**Responsive area illumination** takes place when an IDS detects suspicious activities and turns on the lights within a specific area. When this type of technology is plugged into automated IDS products, there is a high likelihood of false alarms. Instead of continuously having to dispatch a security guard to check out these issues, a CCTV camera can be installed to scan the area for intruders.

If intruders want to disrupt the security personnel or decrease the probability of being seen while attempting to enter a company’s premises or building, they could attempt to turn off the lights or cut power to them. This is why lighting controls and switches should be in protected, locked, and centralized areas.

**Surveillance Devices**

Usually, installing fences and lights does not provide the necessary level of protection a company needs to protect its facility, equipment, and employees. Areas need to be under surveillance so improper actions are noticed and taken care of before damage occurs. Surveillance can happen through visual detection or through devices that use sophisticated means of detecting abnormal behavior or unwanted conditions. It is important that every organization have a proper mix of lighting, security personnel, IDSs, and surveillance technologies and techniques.
Visual Recording Devices

Because surveillance is based on sensory perception, surveillance devices usually work in conjunction with guards and other monitoring mechanisms to extend their capabilities and range of perception. A closed-circuit TV (CCTV) system is a commonly used monitoring device in most organizations, but before purchasing and implementing a CCTV, you need to consider several items:

- **The purpose of CCTV**  To detect, assess, and/or identify intruders
- **The type of environment the CCTV camera will work in**  Internal or external areas
- **The field of view required**  Large or small area to be monitored
- **Amount of illumination of the environment**  Lit areas, unlit areas, areas affected by sunlight
- **Integration with other security controls**  Guards, IDSs, alarm systems

The reason you need to consider these items before you purchase a CCTV product is that there are so many different types of cameras, lenses, and monitors that make up the different CCTV products. You must understand what is expected of this physical security control, so you purchase and implement the right type.

CCTVs are made up of cameras, transmitters, receivers, a recording system, and a monitor. The camera captures the data and transmits it to a receiver, which allows the data to be displayed on a monitor. The data are recorded so they can be reviewed at a later time if needed. Figure 6-20 shows how multiple cameras can be connected to one multiplexer, which allows several different areas to be monitored at one time. The multiplexer accepts video feed from all the cameras and interleaves these transmissions over one line to the central monitor. This is more effective and efficient than the older systems that require the security guard to physically flip a switch from one environment to the next. In these older systems, the guard can view only one environment at a time, which of course makes it more likely that suspicious activities will be missed.

A CCTV sends the captured data from the camera’s transmitter to the monitor’s receiver, usually through a coaxial cable, instead of broadcasting the signals over a public network. This is where the term “closed-circuit” comes in. This circuit should be tamperproof, which means an intruder cannot manipulate the video feed that the security guard is monitoring. The most common type of attack is to replay previous recordings without the security personnel knowing it. For example, if an attacker is able to compromise a company’s CCTV and play the recording from the day before, the security guard would not know an intruder is in the facility carrying out some type of crime. This is one reason why CCTVs should be used in conjunction with intruder detection controls, which we address in the next section.

**NOTE**  CCTVs should have some type of recording system. Digital recorders save images to hard drives and allow advanced search techniques that are not possible with videotape recorders. Digital recorders use advanced compression techniques, which drastically reduce the storage media requirements.
Most of the CCTV cameras in use today employ light-sensitive chips called charged-coupled devices (CCDs). The CCD is an electrical circuit that receives input light from the lens and converts it into an electronic signal, which is then displayed on the monitor. Images are focused through a lens onto the CCD chip surface, which forms the electrical representation of the optical image. It is this technology that allows for the capture of extraordinary detail of objects and precise representation, because it has sensors that work in the infrared range, which extends beyond human perception. The CCD sensor picks up this extra “data” and integrates it into the images shown on the monitor to allow for better granularity and quality in the video.

CCDs are also used in fax machines, photocopiers, bar code readers, and even telescopes. CCTVs that use CCDs allow more granular information within an environment to be captured and shown on the monitor when compared to the older CCTV technology that relied upon cathode ray tubes (CRTs).

Two main types of lenses are used in CCTV: fixed focal length and zoom (varifocal). The focal length of a lens defines its effectiveness in viewing objects from a horizontal and vertical view. The focal length value relates to the angle of view that can be achieved. Short focal length lenses provide wider-angle views, while long focal length lenses provide a narrower view. The size of the images shown on a monitor, along with the area covered by one camera, is defined by the focal length. For example, if a company implements a CCTV camera in a warehouse, the focal length lens values should be between 2.8 and 4.3 millimeters (mm) so the whole area can be captured. If the company implements another CCTV camera that monitors an entrance, that lens value should be around 8mm, which allows a smaller area to be monitored.
NOTE Fixed focal length lenses are available in various fields of views: wide, medium, and narrow. A lens that provides a “normal” focal length creates a picture that approximates the field of view of the human eye. A wide-angle lens has a short focal length, and a telephoto lens has a long focal length. When a company selects a fixed focal length lens for a particular view of an environment, it should understand that if the field of view needs to be changed (wide to narrow), the lens must be changed.

So, if we need to monitor a large area, we use a lens with a smaller focal length value. Great, but what if a security guard hears a noise or thinks he sees something suspicious? A fixed focal length lens is stationary, meaning the guard cannot move the camera from one point to the other and properly focus the lens automatically. The zoom lenses provide flexibility by allowing the viewer to change the field of view to different angles and distances. The security personnel usually have a remote-control component integrated within the centralized CCTV monitoring area that allows them to move the cameras and zoom in and out on objects as needed. When both wide scenes and close-up captures are needed, a zoom lens is best. This type of lens allows the focal length to change from wide angle to telephoto while maintaining the focus of the image.

To understand the next characteristic, depth of field, think about pictures you might take while on vacation with your family. For example, if you want to take a picture of your spouse with the Grand Canyon in the background, the main object of the picture is your spouse. Your camera is going to zoom in and use a shallow depth of focus. This provides a softer backdrop, which will lead the viewers of the photograph to the foreground, which is your spouse. Now, let’s say you get tired of taking pictures of your spouse and want to get a scenic picture of just the Grand Canyon itself. The camera would use a greater depth of focus, so there is not such a distinction between objects in the foreground and background.

The depth of field is necessary to understand when choosing the correct lenses and configurations for your company’s CCTV. The depth of field refers to the portion of the environment that is in focus when shown on the monitor. The depth of field varies depending upon the size of the lens opening, the distance of the object being focused on, and the focal length of the lens. The depth of field increases as the size of the lens opening decreases, the subject distance increases, or the focal length of the lens decreases. So, if you want to cover a large area and not focus on specific items, it is best to use a wide-angle lens and a small lens opening.

CCTV lenses have irises, which control the amount of light that enters the lens. Manual iris lenses have a ring around the CCTV lens that can be manually turned and controlled. A lens with a manual iris would be used in areas that have fixed lighting, since the iris cannot self-adjust to changes of light. An auto iris lens should be used in environments where the light changes, as in an outdoor setting. As the environment brightens, this is sensed by the iris, which automatically adjusts itself. Security personnel will configure the CCTV to have a specific fixed exposure value, which the iris is responsible for maintaining. On a sunny day, the iris lens closes to reduce the amount of light entering the camera, while at night, the iris opens to capture more light—just like our eyes.
When choosing the right CCTV for the right environment, you must determine the amount of light present in the environment. Different CCTV camera and lens products have specific illumination requirements to ensure the best quality images possible. The illumination requirements are usually represented in the lux value, which is a metric used to represent illumination strengths. The illumination can be measured by using a light meter. The intensity of light (illumination) is measured and represented in measurement units of lux or footcandles. (The conversion between the two is one footcandle = 10.76 lux.) The illumination measurement is not something that can be accurately provided by the vendor of a light bulb, because the environment can directly affect the illumination. This is why illumination strengths are most effectively measured where the light source is implemented.

Next, you need to consider the mounting requirements of the CCTV cameras. The cameras can be implemented in a fixed mounting or a mounting that allows the cameras to move when necessary. A fixed camera cannot move in response to security personnel commands, whereas cameras that provide PTZ capabilities can pan, tilt, or zoom as necessary.

So, buying and implementing a CCTV system may not be as straightforward as it seems. As a security professional, you would need to understand the intended use of the CCTV, the environment that will be monitored, and the functionalities that will be required by the security staff that will use the CCTV on a daily basis. The different components that can make up a CCTV product are shown in Figure 6-21.

Great—your assessment team has done all of its research and bought and implemented the correct CCTV system. Now it would be nice if someone actually watched the monitors for suspicious activities. Realizing that monitor watching is a mentally deadening activity may lead your team to implement a type of annuciator system. Different types of annuciator products are available that can either “listen” for noise and activate electrical devices, such as lights, sirens, or CCTV cameras, or detect movement. Instead of expecting a security guard to stare at a CCTV monitor for eight hours straight, the guard can carry out other activities and be alerted by an annuciator if movement is detected on a screen.

Intrusion Detection Systems

Surveillance techniques are used to watch for unusual behaviors, whereas intrusion detection devices are used to sense changes that take place in an environment. Both are monitoring methods, but they use different devices and approaches. This section addresses the types of technologies that can be used to detect the presence of an intruder. One such machine, a perimeter scanning device, is shown in Figure 6-22.

IDSs are used to detect unauthorized entries and alert a responsible entity to respond. These systems can monitor entries, doors, windows, devices, or removable coverings of equipment. Many work with magnetic contacts or vibration-detection devices that are sensitive to certain types of changes in the environment. When a change is detected, the IDS device sounds an alarm either in the local area, or in both the local area and a remote police or guard station.
Figure 6-21 A CCTV product can be comprised of several components.

Figure 6-22 Different perimeter scanning devices work by covering a specific area.
IDSs can be used to detect changes in the following:

- Beams of light
- Sounds and vibrations
- Motion
- Different types of fields (microwave, ultrasonic, electrostatic)
- Electrical circuit

IDSs can be used to detect intruders by employing electromechanical systems (magnetic switches, metallic foil in windows, pressure mats) or volumetric systems. Volumetric systems are more sensitive because they detect changes in subtle environmental characteristics, such as vibration, microwaves, ultrasonic frequencies, infrared values, and photoelectric changes.

**Electromechanical systems** work by detecting a change or break in a circuit. The electrical circuits can be strips of foil embedded or connected to windows. If the window breaks, the foil strip breaks, which sounds an alarm. Vibration detectors can detect movement on walls, screens, ceilings, and floors when the fine wires embedded within the structure are broken. Magnetic contact switches can be installed on windows and doors. If the contacts are separated because the window or door is opened, an alarm will sound.

Another type of electromechanical detector is a pressure pad. This is placed underneath a rug or portion of the carpet and is activated after hours. If someone steps on the pad, an alarm initiates, because no one is supposed to be in this area during this time.

Types of volumetric IDSs are photoelectric, acoustical-seismic, ultrasonic, and microwave.

A **photoelectric system** (or photometric system) detects the change in a light beam and thus can be used only in windowless rooms. These systems work like photoelectric smoke detectors, which emit a beam that hits the receiver. If this beam of light is interrupted, an alarm sounds. The beams emitted by the photoelectric cell can be cross-sectional and can be invisible or visible beams. Cross-sectional means that one area can have several different light beams extending across it, which is usually carried out by using hidden mirrors to bounce the beam from one place to another until it hits the light receiver. These are the most commonly used systems in the movies. You have probably seen James Bond and other noteworthy movie spies or criminals use night-vision goggles to see the invisible beams and then step over them.

A **passive infrared system (PIR)** identifies the changes of heat waves in an area it is configured to monitor. If the particles’ temperature within the air rises, it could be an indication of the presence of an intruder, so an alarm is sounded.

An **acoustical detection system** uses microphones installed on floors, walls, or ceilings. The goal is to detect any sound made during a forced entry. Although these systems are easily installed, they are very sensitive and cannot be used in areas open to sounds of storms or traffic. **Vibration sensors** are very similar and are also implemented to detect forced entry. Financial institutions may choose to implement these types of sensors on exterior walls, where bank robbers may attempt to drive a vehicle through. They are also commonly used around the ceiling and flooring of vaults to detect someone trying to make an unauthorized bank withdrawal.
Wave-pattern motion detectors range in the frequency of the waves they monitor. The different frequencies are microwave, ultrasonic, and low frequency. All of these devices generate a wave pattern that is sent over a sensitive area and reflected back to a receiver. If the pattern is returned undisturbed, the device does nothing. If the pattern returns altered, because something in the room is moving, an alarm sounds.

A proximity detector, or capacitance detector, emits a measurable magnetic field. The detector monitors this magnetic field, and an alarm sounds if the field is disrupted. These devices are usually used to protect specific objects (artwork, cabinets, or a safe) versus protecting a whole room or area. Capacitance change in an electrostatic field can be used to catch a bad guy, but first you need to understand what capacitance change means. An electrostatic IDS creates an electrostatic magnetic field, which is just an electric field associated with static electric charges. All objects have a static electric charge. They are all made up of many subatomic particles, and when everything is stable and static, these particles constitute one holistic electric charge. This means there is a balance between the electric capacitance and inductance. Now, if an intruder enters the area, his subatomic particles will mess up this lovely balance in the electrostatic field, causing a capacitance change, and an alarm will sound. So if you want to rob a company that uses these types of detectors, leave the subatomic particles that make up your body at home.

The type of motion detector that a company chooses to implement, its power capacity, and its configurations dictate the number of detectors needed to cover a sensitive area. Also, the size and shape of the room and the items within the room may cause barriers, in which case more detectors would be needed to provide the necessary level of coverage.

IDSs are support mechanisms intended to detect and announce an attempted intrusion. They will not prevent or apprehend intruders, so they should be seen as an aid to the organization’s security forces.

**Intrusion Detection Systems Characteristics**

IDSs are very valuable controls to use in every physical security program, but several issues need to be understood before their implementation.

- They are expensive and require human intervention to respond to the alarms.
- A redundant power supply and emergency backup power are necessary.
- They can be linked to a centralized security system.
- They should have a fail-safe configuration, which defaults to “activated.”
- They should detect, and be resistant to, tampering.

**Patrol Force and Guards**

One of the best security mechanisms is a security guard and/or a patrol force to monitor a facility’s grounds. This type of security control is more flexible than other security mechanisms, provides good response to suspicious activities, and works as a great deterrent. However, it can be a costly endeavor, because it requires a salary, benefits, and time off. People sometimes are unreliable. Screening and bonding is an important part of selecting a security guard, but this only provides a certain level of assurance.
IDSs and physical protection measures ultimately require human intervention. Security guards can be at a fixed post or can patrol specific areas. Different organizations will have different needs from security guards. They may be required to check individual credentials and enforce filling out a sign-in log. They may be responsible for monitoring IDSs and expected to respond to alarms. They may need to issue and recover visitor badges, respond to fire alarms, enforce rules established by the company within the building, and control what materials can come into or go out of the environment. The guard may need to verify that doors, windows, safes, and vaults are secured; report identified safety hazards; enforce restrictions of sensitive areas; and escort individuals throughout facilities.

The security guard should have clear and decisive tasks that she is expected to fulfill. The guard should be fully trained on the activities she is expected to perform and on the responses expected from her in different situations. She should also have a central control point to check in to, two-way radios to ensure proper communication, and the necessary access into areas she is responsible for protecting.

The best security has a combination of security mechanisms and does not depend on just one component of security. Thus, a security guard should be accompanied by other surveillance and detection mechanisms.

**Dogs**

Dogs have proven to be highly useful in detecting intruders and other unwanted conditions. Their hearing and sight outperform those of humans, and their intelligence and loyalty can be used for protection.

The best security dogs go through intensive training to respond to a wide range of commands and to perform many tasks. Dogs can be trained to hold an intruder at bay until security personnel arrive or to chase an intruder and attack. Some dogs are trained to smell smoke so they can alert others to a fire.

Of course, dogs cannot always know the difference between an authorized person and an unauthorized person, so if an employee goes into work after hours, she can have more on her hands than expected. Dogs can provide a good supplementary security mechanism, or a company can ask the security guard to bare his teeth at the sight of an unknown individual instead. Whatever works.

**Auditing Physical Access**

Physical access control systems can use software and auditing features to produce audit trails or access logs pertaining to access attempts. The following information should be logged and reviewed:

- The date and time of the access attempt
- The entry point at which access was attempted
- The user ID employed when access was attempted
- Any unsuccessful access attempts, especially if during unauthorized hours
As with audit logs produced by computers, access logs are useless unless someone actually reviews them. A security guard may be required to review these logs, but a security professional or a facility manager should also review these logs periodically. Management needs to know where entry points into the facility exist and who attempts to use them.

Audit and access logs are detective, not preventive. They are used to piece together a situation after the fact instead of attempting to prevent an access attempt in the first place.

**Testing and Drills**

Having fire detectors, portable extinguishers, and suppressions agents are great, but people also need to be properly trained on what to do when a fire (or other type of emergency) takes place. An evacuation and emergency response plan must be developed and actually put into action. It needs to be documented and put in places that are easily accessible in times of crisis. The people who are assigned specific tasks must be taught and informed how to fulfill those tasks, and dry runs must be done to walk people through different emergency situations. The drills should take place at least once a year, and the entire program should be continually updated and improved.

The tests and drills prepare personnel for what they may be faced with and provide a controlled environment to learn the tasks expected of them. These tests and drills also point out issues that may not have been previously thought about and addressed in the planning process.

The exercise should have a predetermined scenario that the company may indeed be faced with one day. Specific parameters and a scope of the exercise must be worked out before sounding the alarms. The team of testers must agree upon what exactly is getting tested and how to properly determine success or failure. The team must agree upon the timing and duration of the exercise, who will participate in the exercise, who will receive which assignments, and what steps should be taken. During evacuation, specific people should be given lists of employees that they are responsible for ensuring they have escaped the building. This is the only way the organization will know if someone is still left inside and who that person is.

- Tests and drills:
  - Prepare personnel
  - Provide a controlled environment
- Evacuation and emergency response plans:
  - Need to be developed
  - Must be put into action
  - Need to be documented
  - Must be put in easily accessible places
  - People must be assigned specific tasks
  - People should be taught and informed how to fulfill those tasks
  - Drills should take place at least once a year
The entire program should be continually updated and improved
Agree upon parameters for drills and tests:
- The timing and duration of the exercise
- Who will participate in the exercise
- Who will receive which assignments
- What steps should be taken

Summary

Our distributed environments have put much more responsibility on the individual user, facility management, and administrative procedures and controls than in the old days. Physical security is not just the night guard who carries around a big flashlight. Now, security can be extremely technical, comes in many forms, and raises many liability and legal issues. Natural disasters, fires, floods, intruders, vandals, environmental issues, construction materials, and power supplies all need to be planned for and dealt with.

Every organization should develop, implement, and maintain a physical security program that contains the following control categories: deterrence, delay, detection, assessment, and response. It is up to the organization to determine its acceptable risk level and the specific controls required to fulfill the responsibility of each category.

Physical security is not often considered when people think of organizational security and company asset protection, but real threats and risks need to be addressed and planned for. Who cares if a hacker can get through an open port on the web server if the building is burning down?

References

- International CPTED Association (ICA)  www.cpted.net

Quick Tips

- Physical security is usually the first line of defense against environmental risks and unpredictable human behavior.
- Crime Prevention Through Environmental Design (CPTED) combines the physical environment and sociology issues that surround it to reduce crime rates and the fear of crime.
- The value of property within the facility and the value of the facility itself need to be ascertained to determine the proper budget for physical security so that security controls are cost-effective.
- Automated environmental controls help minimize the resulting damage and speed the recovery process. Manual controls can be time-consuming and error prone, and require constant attention.
Physical construction materials and structure composition need to be evaluated for their protective characteristics, their utility, and their costs and benefits.

Some physical security controls may conflict with the safety of people. These issues need to be addressed; human life is always more important than protecting a facility or the assets it contains.

When looking at locations for a facility, consider local crime, natural disaster possibilities, and distance to hospitals, police and fire stations, airports, and railroads.

The HVAC system should maintain the appropriate temperature and humidity levels, provide closed-loop recirculating air conditioning, and positive pressurization and ventilation.

High humidity can cause corrosion, and low humidity can cause static electricity.

Dust and other air contaminants may adversely affect computer hardware, and should be kept to acceptable levels.

Administrative controls include drills and exercises of emergency procedures, simulation testing, documentation, inspections and reports, prescreening of employees, post-employment procedures, delegation of responsibility and rotation of duties, and security-awareness training.

Emergency procedure documentation should be readily available and periodically reviewed and updated.

Proximity identification devices can be user-activated (action needs to be taken by a user) or system sensing (no action needs to be taken by the user).

A transponder is a proximity identification device that does not require action by the user. The reader transmits signals to the device, and the device responds with an access code.

Exterior fencing can be costly and unsightly, but can provide crowd control and help control access to the facility.

Interior partitions may not go all the way up to the ceiling; therefore, an intruder can remove a ceiling tile and climb over the partition into a critical portion of the facility.

Intrusion detection devices include motion detectors, CCTVs, vibration sensors, and electromechanical devices.

Intrusion detection devices can be penetrated, are expensive to install and monitor, require human response, and are subject to false alarms.

CCTV enables one person to monitor a large area, but should be coupled with alerting functions to ensure proper response.

Security guards are expensive but provide flexibility in response to security breaches and can deter intruders from attempting an attack.

A cipher lock uses a keypad and is programmable.

Company property should be marked as such, and security guards should be trained how to identify when these items leave the facility in an improper manner.
Media should be protected from destruction, modification, theft, unauthorized copying, and disclosure.

Floors, ceilings, and walls need to be able to hold the necessary load and provide the required fire rating.

Water, steam, and gas lines need to have shutoff valves and positive drains (substance flows out instead of in).

The threats to physical security are interruption of services, theft, physical damage, unauthorized disclosure, and loss of system integrity.

The primary power source is what is used in day-to-day operations, and the alternate power source is a backup in case the primary source fails.

Power companies usually plan and implement brownouts when they are experiencing high demand.

Power noise is a disturbance of power and can be caused by electromagnetic interference (EMI) or radio frequency interference (RFI).

EMI can be caused by lightning, motors, and the current difference between wires. RFI can be caused by electrical system mechanisms, fluorescent lighting, and electrical cables.

Power transient noise is disturbance imposed on a power line that causes electrical interference.

Power regulators condition the line to keep voltage steady and clean.

UPS factors that should be reviewed are the size of the electrical load the UPS can support, the speed with which it can assume the load when the primary source fails, and the amount of time it can support the load.

Shielded lines protect from electrical and magnetic induction, which causes interference to the power voltage.

Perimeter protection is used to deter trespassing and to enable people to enter a facility through a few controlled entrances.

Smoke detectors should be located on and above suspended ceilings, below raised floors, and in air ducts to provide maximum fire detection.

A fire needs high temperatures, oxygen, and fuel. To suppress it, one or more of those items needs to be reduced or eliminated.

Gases, like halon, FM-200, and other halon substitutes, interfere with the chemical reaction of a fire.

The HVAC system should be turned off before activation of a fire suppressant to ensure it stays in the needed area and smoke is not distributed to different areas of the facility.

Portable fire extinguishers should be located within 50 feet of electrical equipment and should be inspected quarterly.

CO₂ is a colorless, odorless, and potentially lethal substance because it removes the oxygen from the air to suppress fires.
Chapter 6: Physical and Environmental Security

- Piggybacking, when unauthorized access is achieved to a facility via another individual’s legitimate access, is a common concern with physical security.
- Halon is no longer available because it depletes the ozone. FM-200 or other similar substances are used instead of halon.
- Proximity systems require human response, can cause false alarms, and depend on a constant power supply, so these protection systems should be backed up by other types of security systems.
- Dry pipe systems reduce the accidental discharge of water because the water does not enter the pipes until an automatic fire sensor indicates there is an actual fire.
- In locations with freezing temperatures where broken pipes cause problems, dry pipes should be used.
- A preaction pipe delays water release.
- CCTVs are best used in conjunction with other monitoring and intrusion alert methods.

Questions

Please remember that these questions are formatted and asked in a certain way for a reason. You must remember that the CISSP exam is asking questions at a conceptual level. Questions may not always have the perfect answer, and the candidate is advised against always looking for the perfect answer. The candidate should look for the best answer in the list.

1. What is the first step that should be taken when a fire has been detected?
   A. Turn off the HVAC system and activate fire door releases.
   B. Determine which type of fire it is.
   C. Advise individuals within the building to leave.
   D. Activate the fire suppression system.

2. A company needs to implement a CCTV system that will monitor a large area outside the facility. Which of the following is the correct lens combination for this?
   A. A wide-angle lens and a small lens opening
   B. A wide-angle lens and a large lens opening
   C. A wide-angle lens and a large lens opening with a small focal length
   D. A wide-angle lens and a large lens opening with a large focal length

3. When should a Class C fire extinguisher be used instead of a Class A fire extinguisher?
   A. When electrical equipment is on fire
   B. When wood and paper are on fire
   C. When a combustible liquid is on fire
   D. When the fire is in an open area
4. Which of the following is not a true statement about CCTV lenses?
   A. Lenses that have a manual iris should be used in outside monitoring.
   B. Zoom lenses will carry out focus functionality automatically.
   C. Depth of field increases as the size of the lens opening decreases.
   D. Depth of field increases as the focal length of the lens decreases.

5. How does halon fight fires?
   A. It reduces the fire’s fuel intake.
   B. It reduces the temperature of the area and cools the fire out.
   C. It disrupts the chemical reactions of a fire.
   D. It reduces the oxygen in the area.

6. What is a mantrap?
   A. A trusted security domain
   B. A logical access control mechanism
   C. A double-door facility used for physical access control
   D. A fire suppression device

7. What is true about a transponder?
   A. It is a card that can be read without sliding it through a card reader.
   B. It is a passive proximity device.
   C. It is a card that a user swipes through a card reader to gain access to a facility.
   D. It exchanges tokens with an authentication server.

8. When is a security guard the best choice for a physical access control mechanism?
   A. When discriminating judgment is required
   B. When intrusion detection is required
   C. When the security budget is low
   D. When access controls are in place

9. Which of the following is not a characteristic of an electrostatic intrusion detection system?
   A. It creates an electrostatic field and monitors for a capacitance change.
   B. It can be used as an intrusion detection system for large areas.
   C. It produces a balance between the electric capacitance and inductance of an object.
   D. It can detect if an intruder comes within a certain range of an object.

10. What is a common problem with vibration-detection devices used for perimeter security?
A. They can be defeated by emitting the right electrical signals in the protected area.
B. The power source is easily disabled.
C. They cause false alarms.
D. They interfere with computing devices.

11. Which of the following is an example of glare protection?
A. Using automated iris lenses with short focal lengths
B. Using standby lighting, which is produced by a CCTV camera
C. Directing light toward entry points and away from a security force post
D. Ensuring that the lighting system uses positive pressure

12. Which of the following is not a main component of CPTED?
A. Natural access control
B. Natural surveillance
C. Territorial reinforcement
D. Target hardening

13. Which problems may be caused by humidity in an area with electrical devices?
A. High humidity causes excess electricity, and low humidity causes corrosion.
B. High humidity causes corrosion, and low humidity causes static electricity.
C. High humidity causes power fluctuations, and low humidity causes static electricity.
D. High humidity causes corrosion, and low humidity causes power fluctuations.

14. What does positive pressurization pertaining to ventilation mean?
A. When a door opens, the air comes in.
B. When a fire takes place, the power supply is disabled.
C. When a fire takes place, the smoke is diverted to one room.
D. When a door opens, the air goes out.

15. Which of the following answers contains a category of controls that does not belong in a physical security program?
A. Deterrence and delaying
B. Response and detection
C. Assessment and detection
D. Delaying and lighting
16. Which is not an administrative control pertaining to emergency procedures?
   A. Intrusion detection systems
   B. Awareness and training
   C. Drills and inspections
   D. Delegation of duties

17. If an access control has a fail-safe characteristic but not a fail-secure characteristic, what does that mean?
   A. It defaults to no access.
   B. It defaults to being unlocked.
   C. It defaults to being locked.
   D. It defaults to sounding a remote alarm instead of a local alarm.

18. Which of the following is not considered a delaying mechanism?
   A. Locks
   B. Defense-in-depth measures
   C. Warning signs
   D. Access controls

19. What are the two general types of proximity identification devices?
   A. Biometric devices and access control devices
   B. Swipe card devices and passive devices
   C. Preset code devices and wireless devices
   D. User-activated devices and system sensing devices

20. Which of the following answers best describes the relationship between a risk analysis, acceptable risk level, baselines, countermeasures, and metrics?
   A. The risk analysis output is used to determine the proper countermeasures required. Baselines are derived to measure these countermeasures. Metrics are used to track countermeasure performance to ensure baselines are being met.
   B. The risk analysis output is used to help management understand and set an acceptable risk level. Baselines are derived from this level. Metrics are used to track countermeasure performance to ensure baselines are being met.
   C. The risk analysis output is used to help management understand and set baselines. An acceptable risk level is derived from these baselines. Metrics are used to track countermeasure performance to ensure baselines are being met.
   D. The risk analysis output is used to help management understand and set an acceptable risk level. Baselines are derived from the metrics. Metrics are used to track countermeasure performance to ensure baselines are being met.
21. Most of today’s CCTV systems use charged-coupled devices. Which of the following is not a characteristic of these devices?
   A. Receives input through the lenses and converts them into an electronic signal
   B. Captures signals in the infrared range
   C. Provides better-quality images
   D. Records data on hard drives instead of tapes

22. Which is not a drawback to installing intrusion detection and monitoring systems?
   A. It’s expensive to install.
   B. It cannot be penetrated.
   C. It requires human response.
   D. It’s subject to false alarms.

23. What is a cipher lock?
   A. A lock that uses cryptographic keys
   B. A lock that uses a type of key that cannot be reproduced
   C. A lock that uses a token and perimeter reader
   D. A lock that uses a keypad

24. If a cipher lock has a door delay option, what does that mean?
   A. After a door is open for a specific period, the alarm goes off.
   B. It can only be opened during emergency situations.
   C. It has a hostage alarm capability.
   D. It has supervisory override capability.

25. Which of the following best describes the difference between a warded lock and a tumbler lock?
   A. A tumbler lock is more simplistic and easier to circumvent than a warded lock.
   B. A tumbler lock uses an internal bolt and a warded lock uses internal cylinders.
   C. A tumbler lock has more components than a warded lock.
   D. A warded lock is mainly used externally and a tumbler lock is used internally.

Answers

1. C. Human life takes precedence. Although the other answers are important steps in this type of situation, the first step is to warn others and save as many lives as possible.

2. A. The depth of field refers to the portion of the environment that is in focus when shown on the monitor. The depth of field varies depending upon the size of the lens opening, the distance of the object being focused on, and the
focal length of the lens. The depth of field increases as the size of the lens opening decreases, the subject distance increases, or the focal length of the lens decreases. So if you want to cover a large area and not focus on specific items, it is best to use a wide-angle lens and a small lens opening.

3. A Class C fire is an electrical fire. Thus, an extinguisher with the proper suppression agent should be used. The following table shows the fire types, their attributes, and suppression methods:

<table>
<thead>
<tr>
<th>Fire Class</th>
<th>Type of Fire</th>
<th>Elements of Fire</th>
<th>Suppression Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Common combustibles</td>
<td>Wood products, paper, and laminates</td>
<td>Water, foam</td>
</tr>
<tr>
<td>B</td>
<td>Liquid</td>
<td>Petroleum products and coolants</td>
<td>Gas, CO₂, foam, dry powders</td>
</tr>
<tr>
<td>C</td>
<td>Electrical</td>
<td>Electrical equipment and wires</td>
<td>Gas, CO₂, dry powders</td>
</tr>
<tr>
<td>D</td>
<td>Combustible metals</td>
<td>Magnesium, sodium, potassium</td>
<td>Dry powder</td>
</tr>
</tbody>
</table>

4. A. Manual iris lenses have a ring around the CCTV lens that can be manually turned and controlled. A lens that has a manual iris would be used in an area that has fixed lighting, since the iris cannot self-adjust to changes of light. An auto iris lens should be used in environments where the light changes, such as an outdoor setting. As the environment brightens, this is sensed by the iris, which automatically adjusts itself. Security personnel will configure the CCTV to have a specific fixed exposure value, which the iris is responsible for maintaining. The other answers are true.

5. C. Halon is a type of gas used to interfere with the chemical reactions between the elements of a fire. A fire requires fuel, oxygen, high temperatures, and chemical reactions to burn properly. Different suppressant agents have been developed to attack each aspect of a fire: CO₂ displaces the oxygen, water reduces the temperature, and soda acid removes the fuel.

6. C. A mantrap is a small room with two doors. The first door is locked; a person is identified and authenticated by a security guard, biometric system, smart card reader, or swipe card reader. Once the person is authenticated and access is authorized, the first door opens and allows the person into the mantrap. The first door locks and the person is trapped. The person must be authenticated again before the second door unlocks and allows him into the facility.

7. A. A transponder is a type of physical access control device that does not require the user to slide a card through a reader. The reader and card communicate directly. The card and reader have a receiver, transmitter, and battery. The reader sends signals to the card to request information. The card sends the reader an access code.

8. A. Although many effective physical security mechanisms are on the market today, none can look at a situation, make a judgment about it, and decide...
what the next step should be. A security guard is employed when a company
needs to have a countermeasure that can think and make decisions in
different scenarios.

9. B. An electrostatic IDS creates an electrostatic field, which is just an electric
field associated with static electric charges. The IDS creates a balanced
electrostatic field between itself and the object being monitored. If an intruder
comes within a certain range of the monitored object, there is capacitance
change. The IDS can detect this change and sound an alarm.

10. C. This type of system is sensitive to sounds and vibrations and detects the
changes in the noise level of an area it is placed within. This level of sensitivity
can cause many false alarms. These devices do not emit any waves; they only
listen for sounds within an area and are considered passive devices.

11. C. When lighting is installed, it should be directed toward areas where
potential intruders would most likely be coming from, and directed away
from the security force posts. For example, lighting should be pointed at gates
or exterior access points, and the guard locations should be in the shadows, or
under a lower amount of illumination. This is referred to as "glare protection"
for the security force.

12. D. Natural access control is the use of the environment to control access to
entry points, such as using landscaping and bollards. An example of natural
surveillance is the construction of pedestrian walkways so there is a clear line
of sight of all the activities in the surroundings. Territorial reinforcement gives
people a sense of ownership of a property, giving them a greater tendency to
protect it. These concepts are all parts of CPTED. Target hardening has to do
with implementing locks, security guards, and proximity devices.

13. B. High humidity can cause corrosion, and low humidity can cause excessive
static electricity. Static electricity can short out devices or cause loss of
information.

14. D. Positive pressurization means that when someone opens a door, the air
goes out and outside air does not come in. If a facility was on fire and the
doors were opened, positive pressure would cause the smoke to go out instead
of being pushed back into the building.

15. D. The categories of controls that should make up any physical security
program are deterrence, delaying, detection, assessment, and response.
Lighting is a control itself, not a category of controls.

16. A. Awareness and training, drills and inspections, and delegation of duties are
all items that have a direct correlation to proper emergency procedures. It is
management’s responsibility to ensure that these items are in place, properly
tested, and carried out. Intrusion detection systems are technical controls.

17. B. A fail-safe setting means that if a power disruption affected the automated
locking system, the doors would default to being unlocked. A fail-secure
configuration means a door would default to being locked if there were any
problems with the power.
18. C. Every physical security program should have delaying mechanisms, which have the purpose of slowing down an intruder in his activities so security personnel can be alerted and arrive at the scene. A warning sign is a deterrence control, not a delaying control.

19. D. A user-activated system requires the user to do something: swipe the card through the reader and/or enter a code. A system sensing device recognizes the presence of the card and communicates with it without the user needing to carry out any activity.

20. B. The physical security team needs to carry out a risk analysis, which will identify the organization’s vulnerabilities, threats, and business impacts. The team should present these findings to management and work with them to define an acceptable risk level for the physical security program. From there, the team should develop baselines (minimum levels of security) and metrics to properly evaluate and determine whether the baselines are being met by the implemented countermeasures. Once the team identifies and implements the countermeasures, the countermeasures’ performance should be continually evaluated and expressed in the previously created metrics. These performance values are compared to the set baselines. If the baselines are continually maintained, then the security program is successful because the company’s acceptable risk level is not being exceeded.

21. D. The CCD is an electrical circuit that receives input light from the lens and converts it into an electronic signal, which is then displayed on the monitor. Images are focused through a lens onto the CCD chip surface, which forms the electrical representation of the optical image. This technology allows the capture of extraordinary details of objects and precise representation because it has sensors that work in the infrared range, which extends beyond human perception. The CCD sensor picks up this extra “data” and integrates it into the images shown on the monitor, to allow for better granularity and quality in the video. CCD does not record data.

22. B. Monitoring and intrusion detection systems are expensive, require someone to respond when they set off an alarm, and, because of their level of sensitivity, can cause several false alarms. Like any other type of technology or device, they have their own vulnerabilities that can be exploited and penetrated.

23. D. Cipher locks, also known as programmable locks, use keypads to control access into an area or facility. The lock can require a swipe card and a specific combination that’s entered into the keypad.

24. A. A security guard would want to be alerted when a door has been open for an extended period. It may be an indication that something is taking place other than a person entering or exiting the door. A security system can have a threshold set so that if the door is open past this period, an alarm sounds.

25. C. The tumbler lock has more pieces and parts than a warded lock. The key fits into a cylinder, which raises the lock metal pieces to the correct height so the bolt can slide to the locked or unlocked position. A warded lock is easier to circumvent than a tumbler lock.