Chapter 10
Physical Security Requirements

THE CISSP TOPICS COVERED IN THIS CHAPTER INCLUDE:

- ✓ **Domain 3.0: Security Architecture and Engineering**
  - 3.8 Apply security principles to site and facility design
  - 3.9 Design site and facility security controls
    - 3.9.1 Wiring closets/intermediate distribution frame
    - 3.9.2 Server rooms/data centers
    - 3.9.3 Media storage facilities
    - 3.9.4 Evidence storage
    - 3.9.5 Restricted and work area security
    - 3.9.6 Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
    - 3.9.7 Environmental issues (e.g., natural disasters, man-made)
    - 3.9.8 Fire prevention, detection, and suppression
    - 3.9.9 Power (e.g., redundant, backup)
- ✓ **Domain 7: Security Operations**
  - 7.14 Implement and manage physical security
    - 7.14.1 Perimeter security controls
    - 7.14.2 Internal security controls

The topic of physical and environmental security is referenced in several domains. The primary occurrences are in Domain 3.0, “Security Architecture and Engineering,” and Domain 7.0, “Security Operations.”

This chapter explores these issues and discusses safeguards and countermeasures to protect against them. You'll often need a disaster recovery plan or a business continuity plan should a severe physical event (such as an explosion, sabotage, or natural disaster) occur. Chapter 3, “Business Continuity Planning,” and Chapter 18, “Disaster Recovery Planning,” cover those topics in detail.

Apply Security Principles to Site and Facility Design

Without control over the physical environment, no collection of administrative, technical, or logical security controls can provide adequate protection. If a malicious person can gain physical access to your facility or equipment, they can do anything, including destruction, disclosure, and alteration.

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

Secure Facility Plan

A *secure facility plan* outlines your organization's security needs and emphasizes methods or mechanisms to employ to provide security. Such a plan is developed through risk assessment and critical path analysis. *Critical path analysis* is a systematic effort to identify relationships between mission-critical applications, processes, and operations and all the necessary supporting elements, both physical and technological. For example, an online store relies on internet access, computer hardware, electricity, temperature control, storage facilities, etc.

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

While examining critical paths, it is also important to evaluate completed or potential technology convergence. *Technology convergence* is the tendency for various technologies, solutions, utilities, and systems to evolve and merge over time. Often, this results in multiple systems performing similar or redundant tasks or one system taking over the features and abilities of another. Although, in some instances, this can result in improved efficiency and cost savings, it can also represent a single point of failure and become a more valuable target for malicious actors and intruders. For example, if voice, video, building control, storage (i.e., network-attached storage [NAS]), and productivity traffic all share a single connection path rather than individual paths, a single act of sabotage to the main connection is all that is required for intruders or thieves to sever external communications.

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

A secure facility plan is based on a layered defense model. Only with overlapping layers of physical security can a reasonable defense be established against would-be intruders. Physical security should be thought of as establishing an obstacle course or gauntlet that attackers have to attempt to work their way through. Thus, security mechanisms are positioned to operate in

series rather than in parallel to optimize the difficulty of breaching the protective infrastructure.

Site Selection

Site selection should be based on the security needs of the organization. Cost, location, and size are important, but addressing security requirements should always take precedence.

Securing assets depends largely on-site security, which involves numerous considerations and situational elements. Site location and construction are crucial in the overall site selection process.

Proximity to other buildings and businesses is a crucial consideration. What attention do they draw, and how does that affect your operation or facility? If a nearby business attracts too many visitors, generates noise, causes vibrations, or handles dangerous materials, they could harm your employees or buildings. Proximity to emergency-response personnel is another issue to consider.

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

Does your organization need to be easily accessed and thus clearly visible? Or would it be a better design not to stand out? *Industrial camouflage* is the attempt to mask or hide a facility's actual function, purpose, or operations by providing a façade presenting a believable or convincing alternative. For example, a data center may present itself as a food-packing facility.

Facility Design

The top priority of security should always be the protection of the life and safety of personnel. To that end, be sure that all facility designs and physical security controls are in compliance with all

applicable laws and regulations. These may include health and safety requirements, building codes, labor restrictions, and more. In the United States, some common regulations to follow in regard to facility security are guidelines and requirements from the Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA). For most organizations, having a facility security officer to assist with the design, implementation, management, and oversight of facility security may be worthwhile.

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

There's also a well-established school of thought on “secure architecture” that's often called *Crime Prevention Through Environmental Design (CPTED)*. First-generation CPTED addresses facility design, landscaping, entrance concepts, campus layouts, lighting, road placement, and traffic management of vehicles and those on foot, while Second-generation CPTED addresses social cohesion. community culture, connectivity, and threshold capacity.

The core principle of CPTED is that the design of the physical environment can be managed, manipulated, and crafted with the intention to create behavioral effects or changes in people present in those areas that result in a reduction of crime as well as a reduction of the fear of crime. Just think of a dark back alley with sunken doorways and several overflowing trash dumpsters; then compare that to a well-lit street with a broad sidewalk with attractive storefronts. Notice the feelings you have about those locations just by thinking about them. CPTED design-guided

locations have an amazing but subtle effect on people's behaviors as well as their perceptions of a location.

CPTED has numerous recommendations and suggestions for improving facility design for security purposes, such as the following:

- Keep planters under 2.5 feet tall—this prevents them from being used to hide behind or as a step to reach a window.
- Keep decorative elements small or far away from the building.
- Locate the data center at the core of the building.
- Provide benches and tables to encourage people to sit and look around; they provide automatic surveillance.
- Mount cameras in full view to act as a deterrent.
- Keep entrances open and clear (i.e., without obstacles like trees or columns) to maintain visibility.
- Keep the number of entrances to a minimum and close off doorways during evenings or weekends when fewer workers are present.
- Provide parking for visitors near the entrance.
- Make delivery access driveways and entrances less visible or noticeable to the public—for example, by positioning them on the back of the building and requiring an alternate road.

First-generation CPTED has four principles: access control, natural surveillance, image and milieu, and territorial control.

Access control is the subtle guidance of those entering and leaving a building through the placement of entranceways, the use of fences and bollards, and the placement of lights. The idea here is to make the entrance point to a building look like an entrance point without having to resort to giant signs saying, "Enter Here!" This can also extend internally by creating security zones to distinguish the general access areas from those of higher security that require certain classifications or job responsibilities

to enter. Those areas of the same access level should be open, inviting, and easy to move around in, but those areas that are restricted or closed off should seem more difficult to access and require more effort and intention of the individual to access.

Natural surveillance is any means to make criminals feel uneasy through the increasing opportunities for them to be observed. This can be accomplished by an open and obstacle-free outside area, especially around entrances, with clear lines of sight. This can be further increased by encouraging workers and even the public to loiter around the area by providing a pleasing landscape (not directly against the buildings) with plenty of seating. Walkways and stairways should be open so that others nearby can easily see if someone is present. All areas should be very well lit, especially at night.

Image refers to the visual elements and aesthetics of an environment. A well-maintained, aesthetically pleasing space tends to project a positive image. This positive image can influence people's behavior and perceptions, making them more likely to engage positively with the environment. Conversely, poorly maintained or neglected spaces may project a negative image, potentially attracting criminal activity. *Milieu* encompasses the broader environment or setting, including the overall ambiance and character of a place. It considers factors such as lighting, landscaping, signage, and the general “feel” of the surroundings. A positive milieu can contribute to a sense of safety and community, whereas a negative or hostile milieu may contribute to feelings of insecurity and vulnerability.

Territorial control is the attempt to make the area feel like an inclusive, caring community. The area should be designed so that it looks cared for and respected, and that it is actively being defended. This can be accomplished with decorations, flags, lighting, landscaping, presentations of company logos, clearly visible building numbers, decorative sidewalks, and other architectural features. This approach may cause intruders to feel like they don't belong and that their activities would be at a higher risk of being detected.

Second-generation CPTED has four principles: social cohesion, community culture, connectivity, and threshold capacity.

Social cohesion refers to the level of connectedness and solidarity within a community. It involves fostering positive relationships among community members. A cohesive community is more likely to be vigilant, look out for one another, and collectively address safety concerns. Second-generation CPTED recognizes the importance of social cohesion in creating a supportive environment that deters crime.

Understanding and respecting the unique *community culture* is essential in second-generation CPTED. This includes considering the values, traditions, and norms that shape the community's identity. Design interventions should align with the community's culture to ensure they are well received and effectively integrated. Respecting cultural diversity contributes to a sense of ownership and pride among community members, fostering a safer and more inclusive environment.

Connectivity involves creating physical and social links within a community. This includes designing spaces that facilitate interaction and communication among residents. Well-connected neighborhoods with clear pathways, parks, and communal spaces promote a sense of belonging and discourage criminal activities by increasing visibility and natural surveillance.

Threshold capacity refers to the ability of a community or neighborhood to absorb and respond to external influences while maintaining its stability and security. Considering the threshold capacity involves assessing how various changes, such as new developments or social programs, might impact the community. Understanding and respecting the threshold capacity help prevent unintended negative consequences that could undermine the safety and well-being of the community.

The International CPTED Association is an excellent source for information on this subject, as is Oscar Newman's book *Creating Defensible Space,* published by the U.S. Department of Housing and Urban Development's Office of Policy Development and Research.

The use of CPTED does not replace the use of actual facility hardening, such as locked doors, security guards, fences, and bollards. However, combining traditional physical barriers and CPTED strategies can provide preventive, detection, and deterrent security.

Implement Site and Facility Security Controls

The grouping of controls named "physical" should probably be called "facility" instead since the controls for protecting a facility include policies, personnel management, computer technology, and physical barriers. So, just calling this grouping physical is not as accurate as it could be, but physical is the accepted terminology.

Administrative physical security controls include facility construction and selection, site management, building design, personnel controls, awareness training, and emergency response and procedures. *Technical physical security controls* include building access controls; intrusion detection; alarms; security cameras; monitoring; heating, ventilation, and air-conditioning (HVAC) power supplies; and fire detection and suppression. *Physical controls for physical security* include fencing, lighting, locks, construction materials, person traps, guard dogs, and security guards.

When designing physical security for an environment, focus on the functional order in which controls should be used. A common order of operations is as follows:

1. Deter
2. Deny
3. Detect
4. Delay
5. Determine
6. Decide

Security controls should be deployed so that initial attempts to access physical assets are *deterred* (boundary restrictions accomplish this). If deterrence fails, then direct access to physical assets should be *denied* (for example, locked vault doors). If denial fails, your system needs to *detect* intrusion (for example, using motion sensors). If the breach is successful, then the intruder should be *delayed* sufficiently in their access attempts to enable authorities to respond (for example, a cable lock on the asset). Security staff or legal authorities should *determine* the cause of the incident or assess the situation to understand what is occurring. Then, based on that assessment, they should *decide* on the response to implement, such as apprehending the intruder or collecting evidence for further investigation.

A cable lock is used to protect smaller devices and equipment by making them more difficult to steal. A cable lock usually isn't an impenetrable security device, since most portable systems are constructed with thin metal and plastic. However, a thief will be reluctant to swipe a cable-locked device, because the damage caused by forcing the cable lock out of the security/lock slot will be obvious when they attempt to pawn or sell the device.

Equipment Failure

Preparing for equipment failure can take many forms. In some non-mission-critical situations, knowing where to purchase replacement parts for a 48-hour replacement timeline is sufficient. In other situations, maintaining on-site replacement parts is mandatory. Remember that the response time in returning a system to a fully functioning state is directly proportional to the cost involved in maintaining such a solution. Costs include storage, transportation, pre-purchasing, and maintaining on-site installation and restoration expertise. In some cases, keeping replacements on-site is not feasible. Establishing a service-level agreement (SLA) with the hardware

vendor is essential for those situations. An SLA clearly defines the response time a vendor will provide during an equipment failure emergency.

Equipment failure is a common cause of a loss of availability. When deciding on strategies to maintain availability, it is often important to understand the criticality of each asset and business process as well as the associated *allowable interruption window (AIW)*, *service delivery objective (SDO)*, and *maximum tolerable downtime/outage (MTD/MTO)* (see Chapters 3 and 18 for more on these concepts). These ranges, boundaries, and objectives help focus on the necessary strategies to maintain availability or at least minimize downtime while optimizing cost efficiency.

Aging hardware should be scheduled for replacement and/or repair. The schedule for such operations should be based on the *mean time to failure (MTTF)* and *mean time to repair (MTTR)* estimates established for each device or on prevailing best organizational practices for managing the hardware life cycle. MTTF is the expected typical functional lifetime of the device given a specific operating environment. Be sure to schedule all devices to be replaced before their MTTF expires. MTTR is the average length of time required to perform a repair on the device. A device can often undergo numerous repairs before a catastrophic failure is expected. An additional measurement is that of the *mean time between failures (MTBF)*. This estimates the time between the first and any subsequent failures. If the MTTF and MTBF values are the same or fairly similar, manufacturers often only list the MTTF to represent both values.

When a device is sent out for repairs, you need to have an alternate solution or a backup device to fill in for the duration of the repair. Often, waiting until a minor failure occurs before a repair is performed is satisfactory, but waiting until a complete failure occurs before replacement is an unacceptable security practice.

Wiring Closets

A *cable plant management policy* defines a facility's physical structure and deployment of network cabling and related devices. A cable plant is the collection of interconnected cables and intermediary devices (such as cross-connects, patch panels, and switches) that establish the physical network. Elements of a cable plant include the following:

- *Entrance facility:* The demarcation point or main distribution frame (MDF) is the entrance point to the building where the cable from the provider connects the internal cable plant.
- *Equipment room:* This is the main wiring closet for the building, often connected to or adjacent to the entrance facility.
- *Backbone distribution system:* This provides wired connections between the equipment and telecommunications rooms, including cross-floor connections.
- *Wiring closet:* This serves the connection needs of a large building's floor or section by providing space for networking equipment and cabling systems. It also serves as the interconnection point between the backbone and horizontal distribution systems. The wiring closet is also known as the *premises wire distribution room*, *main distribution frame (MDF)*, *intermediate distribution frame (IDF),* and *telecommunications room*.
- *Horizontal distribution system:* This connects the telecommunications room and work areas, often including cabling, cross-connection blocks, patch panels, and supporting hardware infrastructure (such as cable trays, cable hangers, and conduits).

Protected cable distribution or *protective distribution systems (PDSs)* are how cables are protected against unauthorized access or harm. The goals of PDSs are to deter violations, detect access

attempts, and otherwise prevent compromise of cables. Elements of PDS implementation can include protective conduits, sealed connections, and regular human inspections. Some PDS implementations require intrusion or compromise detection within the conduits.

Wiring closets or equipment rooms are commonly used to house and manage the wiring for many other important elements of a building, including alarm systems, circuit breaker panels, telephone punch-down blocks, wireless access points, telephone services, and video systems, including security cameras.

Cable plant security is fundamental. Most of the security for a facility focuses on preventing physical unauthorized access. If an unauthorized intruder gains access to the area, they may be able to steal equipment, pull or cut cables, or even plant a listening device. Thus, the security policy for the building should include a few ground rules, such as the following:

- Never use a wiring closet or equipment room as a general storage area.
- Have adequate locks, which might include biometric elements.
- Keep the area tidy.
- Do not store flammable items in the area.
- Set up video surveillance to monitor activity inside the wiring closet.
- Use a door-open sensor to log entries.
- Do not give keys to anyone except the authorized administrator.
- Perform regular physical inspections of the wiring closet's security and contents.
- Include the entire cable plant in the organization's environmental management and monitoring processes to ensure appropriate environmental control and monitoring,

as well as to detect damaging conditions such as flooding or fire.

It is also essential to notify your building management of your cable plant security policy and access restrictions. Doing so will further reduce unauthorized access attempts.

Server Rooms/Data Centers

Server rooms, *data centers*, communications rooms, *server vaults*, and *IT closets* are enclosed, restricted, and protected rooms where your mission-critical servers and network devices are housed. A server room is often configured as a lights-out area, which is generally designed to improve efficiency. A server room is often not optimized for workers but for housing equipment. Data centers can include gas-based halon-substitute oxygen-displacement fire detection and extinguishing systems, walls with a one-hour minimum fire rating, low temperatures, and little or no lighting (i.e., a lights-out area). Server rooms should be designed to support the optimal operation of the IT infrastructure and to block unauthorized human access or intervention.

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

For many organizations, their data center and their server room are one and the same. For some organizations, a data center is an external location used to house the bulk of their backend computer servers, data storage equipment, and network management equipment. This could be a separate building near the primary offices, or it could be a remote location. A data center might be owned and managed exclusively by your organization, or it could be a leased service from a data center provider (such as a cloud service provider (CSP) or colocation center). A data center could be a single-tenant configuration or a multitenant configuration.

In many data centers and server rooms, a variety of technical controls are employed as access control mechanisms to manage physical access. These include but are not limited to smart/dumb cards, proximity devices and readers biometrics, intrusion detection systems (IDSs) (focusing on physical intruders), and a design based on in-depth defense.

Smartcards and Badges

Badges, *identification cards*, and *security IDs* are forms of physical identification and/or electronic access control devices. A badge can be as simple as a name tag indicating whether you are a valid employee or a visitor (sometimes called a "dumb card"). Or it can be as complex as a smartcard or token device that employs multifactor authentication (MFA) to verify and prove your identity and provide authentication and authorization to access a facility, specific rooms, or secured workstations. Badges may be color-coded by facility or classification level, and they often include pictures, magnetic stripes, QR codes or bar codes for optical decoding, smartcard chips, RFID, NFC, and personal details to help a security guard verify identity.

Smartcards are credit card–sized IDs, badges, or security passes with an embedded magnetic stripe, bar code, or integrated circuit chip. They contain information about the authorized bearer that can be used for identification and/or authentication purposes. Some smartcards can even process information or store reasonable amounts of data in a memory chip. Several phrases or terms may be used when referring to a smartcard:

- An identity token containing integrated circuits (ICs)
- A processor IC card
- An IC card with an *ISO 7816 interface* (Figure 10.1)

FIGURE 10.1 A smartcard's ISO 7816 interface

Smartcards are often viewed as a reliable security solution, but they should not be considered complete by themselves. Smartcards represent a “something you have” authentication factor. Like any single security mechanism, smartcards are subject to weaknesses and vulnerabilities. Smartcards can fall prey to physical, logical, Trojan horse, or social engineering attacks. In most cases, a smartcard is used in a multifactor configuration. Thus, theft or loss of a smartcard does not result in easy impersonation. Smartcards can serve dual (or multiple) purposes, such as gaining access to a facility just by waving the card near a wall-mounted reader or gaining access to a computer system by inserting the card into a reader (which is usually followed by a prompt for a personal identification number [PIN] or other authentication factor—i.e., MFA).

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

A badge can be used either for identification or for authentication. When a badge is used for identification, it is swiped by a device, and then the badge owner must provide one or more authentication factors, such as a password, passphrase, or biological trait (if a biometric device is used). When a badge is used for authentication, the badge owner provides an ID, username, and so on and then swipes the badge to authenticate.

When an employee is terminated or otherwise departs the organization, badges should be retrieved and destroyed as part of the offboarding process. Facility security may require that each authorized person wear badges in plain view. Badges should be designed with security features to minimize the ability of intruders to replicate or duplicate. Day passes and/or visitor badges should be clearly marked as such with bright colors for easy recognition from a distance, especially for escort-required visitors.

Proximity Devices

In addition to smartcards, proximity devices can be used to control physical access. A *proximity device* can be a passive device, a field-powered device, or a transponder. The proximity device is worn or held by the authorized bearer. When it passes near a proximity reader, the reader device is able to determine who the bearer is and whether they have authorized access.

The *passive proximity device* has no active electronics; it is just a small magnet with specific properties (like antitheft devices commonly found in or on retail product packaging). A passive device reflects or otherwise alters the electromagnetic (EM) field

generated by the reader device. This alteration is detected by the reader device, which triggers the alarm, records a log event, or sends a notification.

A *field-powered proximity device* has electronics that activate when the device enters the EM field that the reader generates. Such devices generate electricity from an EM field to power themselves (such as card readers that only require the access card to be waved within inches of the reader to unlock doors). This is effectively radio-frequency identification (RFID); see Chapter 11, "Secure Network Architecture and Components," for more.

A *transponder proximity device* is self-powered and transmits a signal received by the reader. This can occur consistently or only at the press of a button (like a garage door opener or car alarm key fob). Such devices may have batteries or capacitors, or may even be solar-powered.

Automatic Request to Exit (AREX) is a security system feature commonly employed in access control systems to automatically signal to unlock a secured door or gate when someone wishes to exit a protected area. This feature enhances security and convenience by automating the exit process. An AREX system typically involves proximity sensors or devices installed near exit points. These devices can include motion detectors, infrared sensors, pressure-sensitive mats, or other technologies that can detect when someone is approaching the exit.

Intrusion Detection Systems

Intrusion detection systems (IDSs) are automated or manual systems designed to detect an attempted physical intrusion, breach, or attack, the use of an unauthorized entry, or the occurrence of some specific event at an unauthorized or abnormal time. Intrusion detection systems used to monitor physical activity may include security guards, automated access

controls, motion detectors, and other specialty monitoring techniques. See Chapter 17, "Preventing and Responding to Incidents," for a discussion of the different type of IDS that is a logical/technical control related to network or host breaches.

Physical intrusion detection systems, also called *burglar alarms*, detect unauthorized activities and notify the authorities (internal security or external law enforcement). The most common type of system uses a simple circuit dry contact switch at entrance points to detect when a door or window has been opened. Some windows may include an internal wire grid or a surface-mounted foil strip that detects when the glass has been broken. Some systems may even use a light beam–based tripwire mechanism to detect entry into a controlled area. This is similar to the safety mechanism located at the bottom of most automatic garage doors. All of these are examples of perimeter breach detection methods. Most IDSs or burglar alarm systems will include both perimeter breach and internal motion-detection methods (see the later sections "Motion Detectors" and "Perimeter Breach Detection"), which in turn may trigger an authority response or an audible alarm (see the later section "Intrusion Alarms").

Two aspects of any intrusion detection and alarm system can cause it to fail: how it gets its power and how it communicates. The detection and alarm mechanisms will not function if the system loses power. Thus, a reliable detection and alarm system has a battery backup with enough stored power for at least 24 hours of operation.

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

system by cutting power, cutting communication cables, or jamming radio signals.

Motion Detectors

A *motion detector*, or *motion sensor*, is a device that senses movement or sound in a specific area, and it is a common element of intruder detection systems. Many types of motion detectors exist, including the following:

- A *digital motion detector* monitors for significant or meaningful changes in the digital pattern of a monitored area. This is effectively a smart security camera.
- *A passive infrared (PIR) or heat-based motion detector* monitors for significant or meaningful changes in a monitored area's heat levels.
- A *wave pattern motion detector* or *microwave motion detector* transmits a consistent low ultrasonic or high microwave frequency signal into a monitored area and monitors for significant or meaningful changes or disturbances in the reflected pattern.
- A *capacitance motion detector* senses changes in the electrical or magnetic field surrounding a monitored object.
- A *photoelectric motion detector* senses changes in visible light levels for the monitored area. Photoelectric motion detectors are usually deployed in internal rooms with no windows and are kept dark.
- A *passive audio motion detector* listens for abnormal sounds in the monitored area.

"Dual-technology sensors" refer to a type of sensor that combines two different technologies (typically IR motion and microwave motion detection) to enhance the accuracy and reliability of detection. These sensors are designed to minimize false alarms and improve overall performance by leveraging the strengths of multiple technologies.

Perimeter Breach Detection

While motion detection mechanisms can be used to monitor for internal movement, they can also be useful to detect when a perimeter is crossed or breached. Numerous perimeter breach detection technologies may be implemented for this purpose, including contact devices and infrared linear beam sensors.

Contact devices detect the opening of a window or door. Often, these are using a balanced magnetic switch (BMS). These are usually small boxes connected to the frame and a door or window. When the door or window is closed, the two BMS items are close enough to each other to keep an electric circuit open based on a magnet pulling on a metal lever. When the door or window is opened, the switch completes once the magnet pulls far enough away to release the lever. A contact device can be directly connected to a contact alarm, so that the instant a door or window is opened, an alarm is triggered.

Infrared linear beam sensors can be used to detect when someone or something crosses through a threshold, opening, or a specific area of a room. These are similar to the safety devices located at the bottom of a garage door. If the beam between the transmitter and receiver is blocked by someone walking through the beam, then the sensor notices the beam break. This could result in sounding an alarm, notifying security guards, or triggering a safety device (such as opening or closing a door).

Intrusion Alarms

Whenever an intrusion detector registers a significant or meaningful change in the environment, it triggers an alarm. An *alarm* is a separate mechanism that triggers a deterrent, a repellent, and/or a notification.

- *Deterrent alarms:* Alarms that trigger deterrents may engage additional locks, shut doors, and so on. Such an alarm aims to make further intrusion or attack more difficult.
- *Repellent alarms:* Alarms that trigger repellents usually sound an audio siren or bell and turn on lights. These kinds of alarms are used to discourage intruders or attackers from continuing their malicious or trespassing activities and force them off the premises.
- *Notification alarms:* Alarms that trigger notification are often silent from the intruder/attacker perspective but record data about the incident and notify administrators, security guards, and law enforcement. A recording of an incident can take the form of log files and/or security camera recordings. A silent alarm aims to bring authorized security personnel to the location of the intrusion or attack in hopes of catching the person(s) committing the unwanted or unauthorized acts.

  Alarms are also categorized by location: local, centralized, or auxiliary.

- *Local alarm system:* Local alarm systems must broadcast an audible alarm signal that can be easily heard from a distance. Additionally, they must be protected from tampering. For a local alarm system to be effective, a security team or guards must be positioned nearby who can respond when the alarm is triggered.
- *Central station system:* The alarm is usually silent locally, but off-site monitoring agents are notified to respond to the security breach. Most residential security systems are of this type. Most central station systems are well-known or national security companies, such as Brinks and ADT. A

proprietary system is similar to a central station system, but the host organization has its own on-site security staff waiting to respond to security breaches.

- *Auxiliary alarm system:* Auxiliary alarm systems can be added to either local or centralized alarm systems. Emergency services are notified to respond to the incident and arrive at the location when the security perimeter is breached. This can include fire, police, and medical services.

Two or more of these types of intrusion and alarm systems can be incorporated into a single solution.

Secondary Verification Mechanisms

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

Security cameras are security mechanisms related to motion detectors, sensors, and alarms. However, a security camera is not an automated detection-and-response system. A security camera usually requires personnel to watch the captured or live video to detect suspicious and malicious activities and to trigger alarms. Security cameras can expand a security guard's effective visible range, increasing the scope of the oversight. A security camera with AI detection capabilities may serve as a primary detection tool, but often, cameras are used as a secondary or follow-up mechanism that is reviewed after a trigger from a primary detection system occurs.

The same logic used for auditing and audit trails is used for a security camera and recorded events. A visible security camera is

a deterrent measure, whereas reviewing recorded events is a detection measure.

Cameras

Video surveillance, video monitoring, closed-circuit television (CCTV), and *security cameras* are all means to deter unwanted activity and create a digital record of the occurrence of events. Cameras should be positioned at exit and entry points. Cameras should also be used to monitor activities around valuable assets and resources as well as to provide additional protection in public areas such as parking structures and walkways.

Closed-circuit television (CCTV) is a security camera system that resides inside an organization's facility and is usually connected to a recording device and monitors for the security guards to view. Most traditional CCTV systems have been replaced by remote-controlled IP cameras (aka security cameras).

Be sure the locations and capabilities of the security cameras are coordinated with the interior and exterior design of the facility. Cameras should be positioned to have clear sight lines of all exterior walls, entrance and exit points, and interior hallways. Security cameras can be overt and obvious to provide a deterrent benefit, or hidden and concealed to provide a detection benefit primarily.

Most security cameras record to local or cloud-based storage. Cameras vary in type, including visible light, infrared, and motion-triggered recording. Some cameras are fixed, whereas others support remote control of automated *pan, tilt, and zoom (PTZ)*.

Some camera systems include a system on a chip (SoC) or embedded components and may be able to perform various specialty functions, such as time-lapse recording, tracking, facial recognition, object detection, or infrared or color-filtered

recording. Such devices may be targeted by attackers, infected by malware, or remotely controlled by malicious actors.

Dummy or decoy cameras can provide deterrence with minimal expense. Many security cameras are network-connectable (i.e., IP cameras), which allows them to be accessed and controlled over a network.

Some cameras or enhanced video surveillance (EVS) systems are capable of object detection, including faces, devices, and weapons. Detection of an object or person could trigger retention of video, notification of security personnel, closing/locking doors, and/or sounding an alarm.

Some cameras are activated through motion recognition. Motion recognition can trigger a retention of video and/or notify security personnel of the event. Some EVSs can even automatically identify individuals and track their motion across the monitored area. This may include gait analysis. *Gait analysis* is the evaluation of the way someone walks as a form of biometric authentication or identification. Each person has a unique walking pattern, which can be used to recognize them. Gait analysis can be used for walking approach authentication as well as intrusion detection. Gait analysis is effectively a biological characteristic that can be used to differentiate between authorized individuals and unauthorized intruders.

Animals, birds, insects, weather, or foliage may fool simple motion recognition or motion-triggered cameras. A secondary verification mechanism should be used to distinguish between a false alarm and an intrusion. Many camera solutions and EVSs can be enhanced using machine learning to improve video monitoring through automation, improved image recognition, and pattern/activity interpretation.

Access Abuses

No matter what form of physical access control is used, a security guard or other monitoring system must be deployed to prevent abuse, such as gaining unauthorized entry. Examples of access abuses of physical access controls include propping open secured

doors or fail-safe exits and bypassing locks or access controls. Impersonation and masquerading are using someone else's security ID to gain entry into a facility. Tailgating and piggybacking are means to gain unauthorized entry by exploiting an authorized person. See Chapter 2, “Personnel Security and Risk Management Concepts,” for a discussion of impersonation, masquerading, tailgating, and piggybacking. Detecting abuses like these can be done by creating audit trails, retaining access logs, using security cameras (see the previous “Cameras” section), and using security guards (see the section “Security Guards and Guard Dogs,” later in this chapter).

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

Media Storage Facilities

Media storage facilities should be designed to store blank media, reusable media, and even installation media securely. Whether hard drives, flash memory devices, optical disks, or tapes, media should be protected against theft and corruption. A locked storage cabinet or closet should be sufficient for this purpose, but a safe can be installed if deemed necessary. New blank media should be secured to prevent someone from stealing it or planting malware on it.

Media that is reused, such as thumb drives, flash memory cards, or portable hard drives, should be protected against theft and data remnant recovery. *Data remnants* are the remaining data

elements left on a storage device after an insufficient sanitization process is used (see Chapter 5, “Protecting Security of Assets”). Standard deletion or formatting processes clear out the directory structure and mark clusters as available for use but leave the original data in the clusters. A simple un-deletion utility or data recovery scanner can often recover access to these files. Restricting access to media and using secure wiping solutions can reduce this risk.

Installation media must be protected against theft and malware planting. This will ensure that when a new installation needs to be performed, the media is available and safe for use.

Here are some means of implementing secure media storage facilities:

- Store media in a locked cabinet or safe rather than an office supply shelf.
- Have a media librarian or custodian who manages access to the locked media cabinet.
- Use a check-in/checkout process to track who retrieves, uses, and returns media from storage.
- For reusable media, when the device is returned, run a secure drive sanitization or *zeroization* (a procedure that erases data by replacing it with meaningless data such as zeroes) process to remove all data remnants.
- Media can also be verified using a hash-based integrity check mechanism to ensure either that valid files remain valid or that a medium has been properly and fully sanitized to retain no remnants of previous use.

A safe is a movable secured container that is not integrated into a building's construction. A vault is a permanent safe or strongroom that is integrated into a building's construction.

For more security-intensive organizations, placing a security notification label on media may be necessary to indicate its use classification or employ RFID/NFC asset tracking tags on media (see Chapter 11). Higher levels of protection could also include fire, flood, electromagnetic field, and temperature monitoring and protection.

Evidence Storage

Evidence storage is quickly becoming a necessity for all businesses, not just law enforcement–related organizations. A key part of incident response is gathering evidence for root cause analysis (see Chapter 17). As cybercrime events continue to increase, it is important to retain logs, audit trails, and other records of digital events. It may also be necessary to retain image copies of drives or snapshots of virtual machines for future comparison. This may be related to internal corporate investigations or law enforcement–based forensic analysis. In either case, preserving datasets that might be used as evidence is essential to the favorable conclusion to a corporate internal investigation or a law enforcement investigation of cybercrime.

Secure evidence storage is likely to involve the following:

- Using a dedicated storage system distinct from the production network
- Potentially keeping the storage system offline when not actively having new datasets transferred to it
- Blocking internet connectivity to and from the storage system
- Tracking all activities on the evidence storage system
- Calculating hashes for all datasets stored on the system
- Limiting access to the security administrator and legal counsel
- Encrypting all datasets stored on the system

There may be additional security requirements for an evidence storage solution based on your local regulations, industry, or contractual obligations. See Chapter 19, “Investigations and Ethics,” for more.

Work Area Security

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

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

A *clean-desk policy* (or clean-desk-space policy) instructs workers how and why to clean off their desks at the end of each work period. In relation to security, such a policy primarily aims to reduce the disclosure of sensitive information. This can include passwords, financial records, medical information, sensitive plans or schedules, and other confidential materials. If, at the end of each day/shift, a worker places all work materials into a lockable desk drawer or file cabinet, this prevents exposure, loss, and/or theft of these materials.

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

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

An example of a secure or restricted work area is the *sensitive compartmented information facility (SCIF)*. An SCIF is often used by government and military agencies, divisions, and contractors to provide a secure environment for highly sensitive data storage and computation. The purpose of an SCIF is to store, view, and update sensitive compartmented information (SCI), which is a type of classified information. An SCIF has restricted access to limit entrance to those individuals with a specific business need and authorization to access the data contained within. This is usually determined by the individual's clearance and SCI approval levels. In most cases, a SCIF is restricted against using or possessing photography, video, or other recording devices in the secured area. An SCIF can be established in a ground-based facility, an aircraft, or a floating platform. It can be a permanent installation or a temporary establishment, and it is typically located within a structure, although an entire structure can be implemented as an SCIF.

Utility Considerations

Reliable operations of IT and continued ability to perform business tasks often depend on consistency in the mundane utilities. The following sections discuss security concerns of power, noise, temperature, and humidity.

Power Considerations

Power supplied by electric companies is not always consistent and clean. Most electronic equipment demands clean power to function properly. Equipment damage from power fluctuations is a common occurrence. Many organizations opt to manage their own power through various means. The first stage or level of power management is using *surge protectors*. However, these only offer protection against power overloads. In the event a spike of power occurs, the surge protector's fuse will trip or blow (i.e., burn out), and all power will be cut off. Surge protectors should be used only when instant termination of electricity will not cause damage to the equipment.

The next level is to use a *power conditioner* or *power-line conditioner*. It is a form of advanced surge protector that is also able to remove or filter line noise.

The third level of power protection is to use an *uninterruptible power supply (UPS)*. A UPS is a type of self-charging battery that can be used to supply consistent, clean power to sensitive equipment. Most UPS devices provide surge protection, power conditioning, and battery-supplied supplemental power. There are two main types of UPSs: double conversion and line interactive. A UPS can also be called a backup UPS or a standby UPS.

A *double conversion UPS* functions by taking power in from the wall outlet, storing it in a battery, pulling power out of it, and then feeding that power to whatever devices are connected. By directing current through its battery, it is able to maintain a consistent, clean power supply to whatever devices are connected to it.

A *line-interactive UPS* has a surge protector, battery charger/inverter, and voltage regulator positioned between the grid power source and the equipment. The battery is not in line under normal conditions. If the grid fails, there is a type of three-position switch that will automatically switch so that power is pulled from the battery through the inverter and voltage regulator to provide power to the equipment. Lower-quality versions of this type of UPS may have a very short moment when power is interrupted. Although most systems should be able to continue operating with this fault, it can be damaging to sensitive devices or cause other equipment to shut down, freeze, or reboot.

The primary purpose of an UPS is the battery-supplied power that can continue to support the operation of electrical devices in the event of power loss or a disconnect from the power grid. A UPS can continue to supply power for minutes or hours, depending on its battery capacity and how much power the equipment attached to it needs (i.e., the load placed on it).

When designing a UPS-based power management solution, consider what systems are critical and thus need continued power versus those that can be allowed to be powered off during any loss of power. This approach can assist with the optimization and distribution of critical power reserves.

Another power option is a large-scale battery backup or a failover battery. This system collects power into a battery but can switch to pulling power from the battery when the power grid fails. Generally, this system is implemented to supply power to an entire building rather than just one or a few devices. Many traditional versions of battery backups were not implemented as a form of UPS, and thus, there was usually a period of time (even if just a moment) of complete power loss to the equipment as the grid source of power failed and a switching event occurred to retrieve power from a battery. Some modern battery backups are implemented more like a UPS so that power is not interrupted. Such battery backups are often associated with solar power or other green or renewable energy solutions. However, they can be used with a grid-only source of power.

The highest level of power protection is the use of *generators*. If maintaining operations for a considerable time despite a brownout or blackout is necessary, on-site electric generators are required. Such generators turn on automatically when a power failure is detected. Most generators operate using a fuel tank of liquid or gaseous propellant that must be maintained to ensure reliability. Electric generators are considered alternate or backup power sources. With sufficient fuel supply, especially if resupply is possible, then a power generator can serve as an alternative power source for a long time.

UPSs should still be used even when a generator is installed to provide continuous alternative power. In this situation, the purpose of the UPS is to provide power long enough to complete a logical shutdown of a system, or until a generator is powered on and provides stable power. It may take a generator several minutes before it is triggered, starts (i.e., turns on), and is warmed up to provide consistent power.

Ideally, power is consistently clean without any fluctuations, but in reality, commercial power suffers from many problems. Here is a list of terms associated with power issues you should know:

- *Fault:* Momentary complete loss of power
- *Blackout:* Prolonged complete loss of power
- *Sag:* Momentary low voltage
- *Brownout*: Prolonged low voltage
- *Spike:* Momentary high voltage
- *Surge:* Prolonged high voltage
- *Inrush:* An initial spike of power usually associated with connecting to a power source
- *Ground:* The wire in an electrical circuit that provides an alternate pathway for electricity to flow safely to the earth (i.e., the ground)

All of these issues can cause problems for electrical equipment. When you're experiencing a power issue, you have to determine

where the fault is occurring. If the issue takes place outside your meter, then it is to be repaired by the power company, whereas any internal issues are your responsibility.

Noise

Noise is power interference through disturbance, interruption, or fluctuation. Noise that is not consistent is labeled as *transient noise*. Noise can cause more than just problems with how equipment functions related to its power source; it can also interfere with the quality of communications, transmissions, and playback. Noise generated by electric current, that is, *electromagnetic interference (EMI)*, can affect data transmission that relies on electromagnetic transport mechanisms, such as telephone, cellular, television, audio, radio, and network connections.

Radio-frequency interference (RFI) is another source of noise and interference that can affect many of the same systems as EMI. A wide range of common electrical appliances generate RFI, including fluorescent lights, electrical cables, electric space heaters, computers, elevators, motors, and electric magnets, so it's important to locate all such equipment when deploying IT systems and infrastructure elements.

Protecting your power supply and equipment from noise is essential to maintaining a productive and functioning environment for your IT infrastructure. Steps to take for this kind of protection include providing sufficient power conditioning, establishing proper grounding, using shielded cables, running cables through shielding conduits, switching to fiber-optic cables for networking, and limiting copper cable exposure to EMI and RFI sources.

Temperature, Humidity, and Static

In addition to power considerations, maintaining the environment involves control over the HVAC mechanisms. Rooms intended primarily to house computers should generally be kept between 59 and 89.6 degrees Fahrenheit (15 and 32 degrees Celsius). However, some extreme environments run their

equipment 20 degrees Fahrenheit lower or higher than this range. The actual temperature is not as important as keeping devices from reaching a temperature that would cause damage and optimizing temperature related to device performance and humidity management. Some devices may operate more efficiently at higher or lower temperatures. Generally, temperature management is optimized using fans, either directly connected to heat sinks on devices, like CPUs, memory banks, or video cards, or indirectly by being part of their chassis or host storage cabinet (such as a rack-mount cabinet). Fans are used to pull warm/hot air off equipment and out of devices and allow it to be replaced by cooler air.

Hot and cold aisles are a means of maintaining optimum operating temperature in large server rooms. The overall technique is to arrange server racks in lines separated by aisles (Figure 10.2). Then, the airflow system is designed so hot, rising air is captured by air-intake vents on the ceiling, whereas cold air is returned in opposing aisles from either the ceiling or the floor. Thus, every other aisle is hot, then cold.

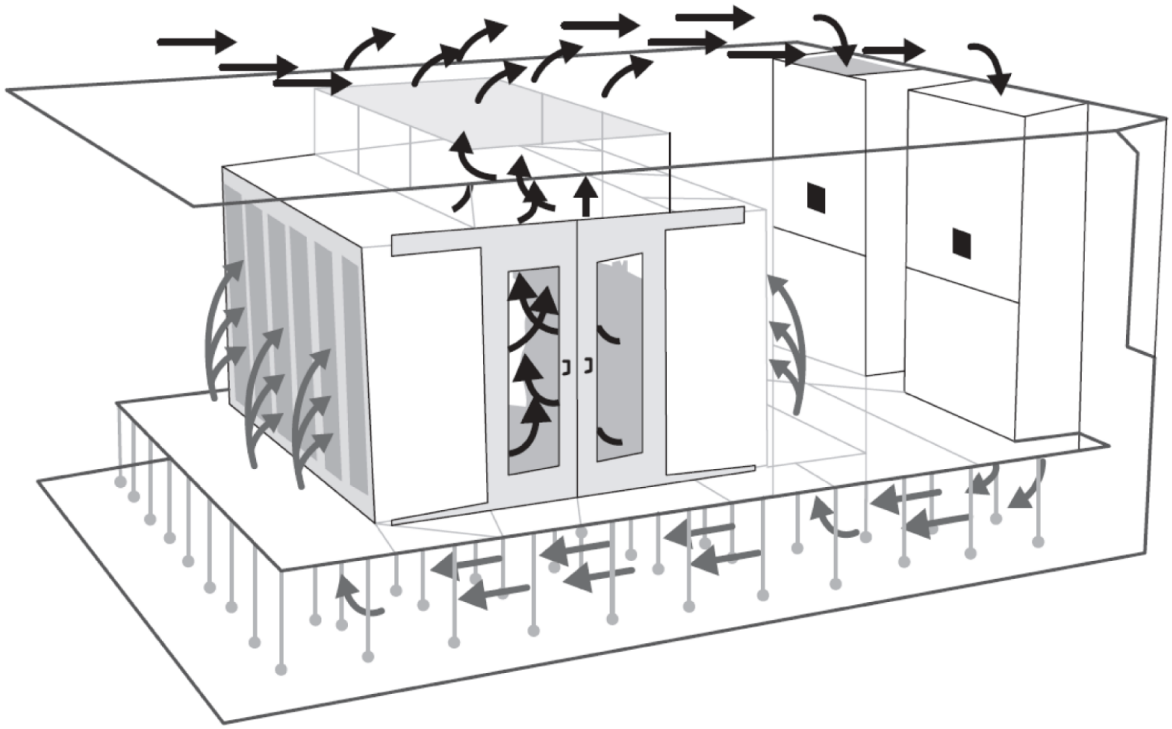

FIGURE 10.2 Hot and cold aisles

A common HVAC-related term is plenum. The plenum consists of boxes and tubes that distribute conditioned air throughout a building. Plenum spaces are the areas of a building designed to contain the HVAC plenum components. Plenum spaces are typically distinct and separate from human-inhabitable spaces within a building. Due to building codes in most countries, anything that is placed into the plenum space must be plenum-rated. This type of fire rating requires that those products produce minimal levels of smoke and/or toxic gases, especially if the building has enclosed spaces that could trap gases. Electrical cables and networking cables are common plenum-rated products.

An important aspect of temperature management is attempting to maintain a stable temperature rather than allowing the temperature to fluctuate up and down. Such heat oscillations can cause the expansion and contraction of materials. This could

cause chip creep (where friction-fit connections work their way out of their sockets) or cracks in soldered connections.

We also recommend that you maintain *positive air pressure* in the data center as well as superior levels of air filtration. These efforts will help reduce dust, debris, microfine particulate matter infiltration, and other contaminants (such as cleaning chemicals or vehicle exhaust). Without such efforts, these unwanted particles can build up over time; dust bunnies can attach to surfaces due to static charges or may cause corrosion.

Additionally, humidity (i.e., relative humidity [RH]) in a computer room should be maintained between 20 and 80 percent. However, some environments allow for RH to be as low as 8 percent and as high as 90 percent. Too much humidity can result in condensation, which causes corrosion. Too little humidity allows for static electricity buildup, which can result in *electrostatic discharge (ESD)*. Even with antistatic carpeting, if the environment has low humidity it is still possible to generate 20,000-volt static discharges from your human body via ESD. Table 10.1 shows that even minimal levels of static discharge can destroy electronic equipment.

TABLE 10.1 Static voltage and damage

Static voltage	Possible damage
40	Destruction of sensitive circuits and other electronic components
1,000	Scrambling of monitor displays
1,500	Destruction of data stored on hard drives
2,000	Abrupt system shutdown
4,000	Printer jam or component damage
17,000	Permanent circuit damage

Environmental monitoring is measuring and evaluating the quality of the environment within a given structure. This can focus on general or basic concerns, such as temperature, humidity, dust, smoke, and other debris. However, more advanced systems can include chemical, biological, radiological, and microbiological detectors.

Condition monitoring is monitoring and assessing the operational parameters, performance, and health of machinery, equipment, or systems in real-time or periodically. The primary goal of condition monitoring is to identify any deviations from normal operating conditions that could indicate potential faults, defects, or deterioration. This proactive approach helps predict and prevent equipment failures, minimize downtime, and optimize maintenance strategies.

Water Issues

Your environmental safety policy and procedures should address water issues, such as leakage and flooding. Plumbing leaks are not an everyday occurrence, but when they do happen, they can cause significant damage.

Water and electricity don't mix. If your computer systems come into contact with water, especially while they are operating, damage is sure to occur. Plus, water and electricity create a serious risk of electrocution for nearby personnel. Whenever possible, locate server rooms, data centers, and critical computer equipment away from any water source or transport pipes located in the building. You may also want to install water-detection circuits on the floor (or under the floor with raised flooring data centers) around mission-critical systems. Water-detection circuits will sound an alarm and alert you if water is encroaching upon the equipment.

To minimize emergencies, be familiar with shutoff valves and drainage locations. In addition to monitoring for plumbing leaks, you should evaluate your facility's ability to handle severe rain or flooding in its vicinity. Is the facility located on a hill or in a valley? Is there sufficient drainage? Is there a history of flooding or accumulation of standing water? Is a server room in the basement or on the first floor? Are there water features or landscaping around the building that might cause flooding or direct heavy rainfall toward and into the building?

Fire Prevention, Detection, and Suppression

Fire prevention, detection, and suppression must not be overlooked. Protecting personnel from harm should always be the most important goal of any security or protection system. In addition to protecting people, fire detection and suppression is designed to keep asset damage caused by fire, smoke, heat, and suppression materials to a minimum.

Standard fire prevention and resolution training involves knowledge of the *fire triangle* (see Figure 10.3). The three corners of the triangle represent fuel, heat, and oxygen. The center of the triangle represents the chemical reaction among these three elements. The purpose of the fire triangle is to illustrate that if you can remove any one of the four items from the fire triangle, the fire can be extinguished. Different suppression mediums address different aspects of the fire:

- Water suppresses the temperature.
- Soda acid and other dry powders suppress the fuel supply.
- Carbon dioxide (CO_2) suppresses the oxygen supply.
- Halon substitutes and other nonflammable gases interfere with the chemistry of combustion and/or suppress the oxygen supply.
- Aqueous film forming foam (AFFF) suppresses temperature and fuel supply.

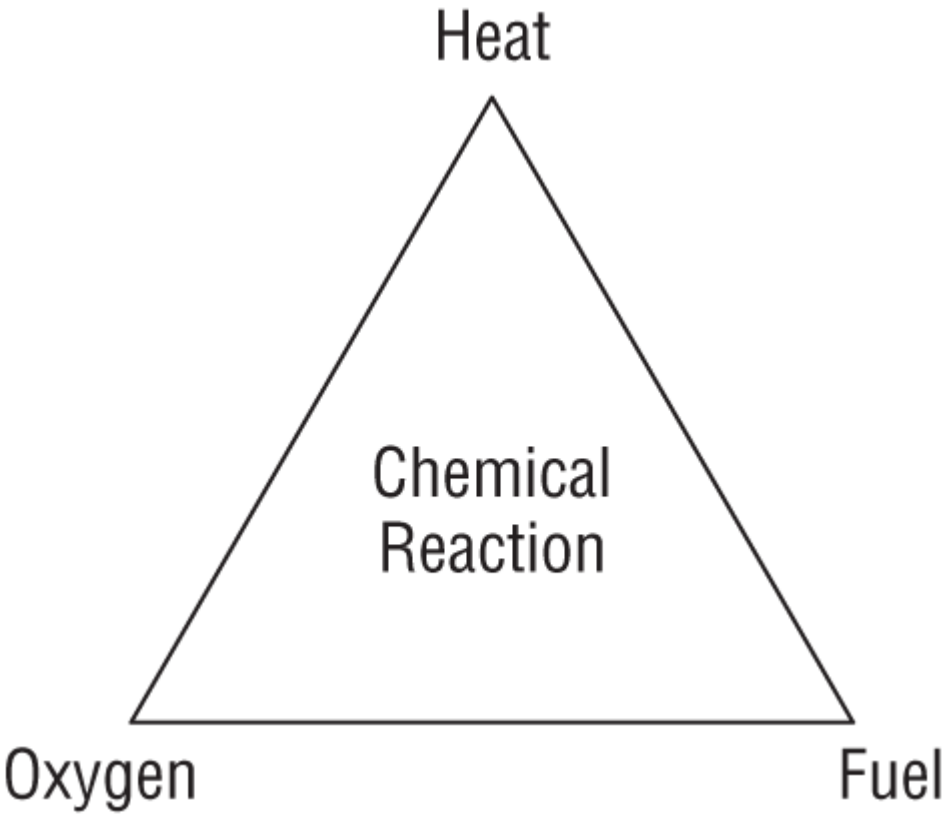

FIGURE 10.3 The fire triangle

Aqueous film forming foam (AFFF) is a type of firefighting foam used to suppress flammable liquid fires. It is a water-based solution containing foaming agents, surfactants, and typically some fluorochemicals. AFFF is designed to quickly spread across the surface of flammable liquids, forming a thin film or barrier that suppresses the release of flammable vapors and prevents the fire from spreading.

When selecting a suppression medium, consider what aspect of the fire triangle it addresses, what this really represents, how effective the suppression medium usually is, and what impact the suppression medium will exert on your environment.

In addition to understanding the fire triangle, you should understand the stages of fire. Fires go through numerous stages, and Figure 10.4 addresses the four most vital stages.

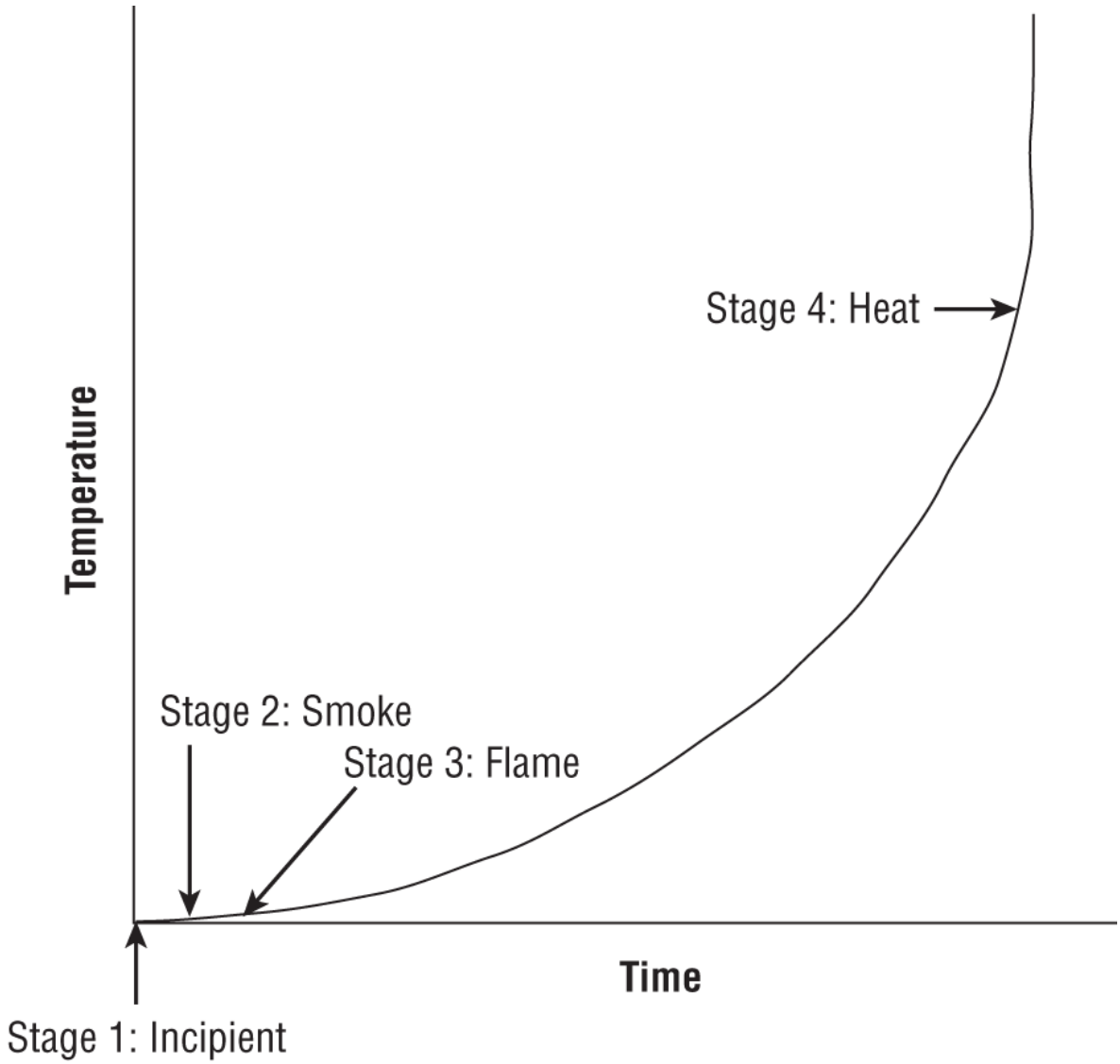

FIGURE 10.4 The four primary stages of fire

Stage 1: The Incipient Stage At this stage, there is only air ionization and no smoke.

Stage 2: The Smoke Stage In Stage 2, smoke is visible from the point of ignition.

Stage 3: The Flame Stage This is when a flame can be seen with the naked eye.

Stage 4: The Heat Stage At Stage 4, the fire is considerably further down the timescale to the point where there is an intense heat buildup and everything in the area burns.

The earlier a fire is detected, the easier it is to extinguish and the less damage it and its suppression medium(s) can cause.

One of the basics of fire management is proper personnel awareness training. Employees need to be trained in safety and escape procedures. Everyone should be thoroughly familiar with the fire suppression mechanisms in their facility. Everyone should also be familiar with at least two evacuation routes from their primary work area and know how to locate evacuation routes elsewhere in the facility. Typically, evacuation routes are indicated by emergency exit signs, illustrated by maps posted on walls, located in common or central areas (such as near elevators), and defined in personnel training and reference manuals. Personnel should be trained in the location and use of fire extinguishers. Organizations should also preestablish a rendezvous location or safety verification mechanism (such as voicemail) to confirm that all employees escaped a building successfully.

Other items to include in fire or general emergency-response training include cardiopulmonary resuscitation (CPR), emergency shutdown procedures, general first aid, and automated external defibrillator (AED) devices.

Once employees are trained, their training should be tested using drills and simulations. All elements of physical security, especially those related to human life and safety, should be tested on a regular basis. It is mandated by law (in the United States) that fire extinguishers, fire detectors/alarms, and elevators be inspected regularly.

Most fires in a data center are caused by overloaded electrical distribution outlets. A second common cause is improper use of heating devices (such as coffeepots, hot plates, and space heaters) when located near combustible materials (such as paper, cloth, and cardboard).

Fire Extinguishers

If a worker notices a fire before the building detects it, then they may be able to use a handheld fire extinguisher to put out the fire. There are several types of fire extinguishers. Understanding what type to use on various forms of fire is essential to effective fire suppression. If a fire extinguisher is used improperly or the wrong form of fire extinguisher is used, the fire could spread and intensify instead of being quenched. A fire extinguisher may be effective through the first three stages of fire, but is unlikely to be of any use at Stage 4, the heat stage.

Fortunately, local fire regulations and building codes typically dictate the type of fire extinguisher to be present. For most standard office environments, a multiclass extinguisher (likely an ABC) is deployed because it is suitable for the widest range of common fire types in that type of location. Table 10.2 lists common types of fire extinguishers.

TABLE 10.2 Fire extinguisher classes

Class	Type	Suppression material
A	Common combustibles	Water, soda acid (a dry powder or liquid chemical)
B	Liquids	AFFF, CO_2, halon or alternate gas options, soda acid
C	Electrical	CO_2, halon or alternate gas options
D	Metals	Dry powder
K	Cooking media (fats, oil)	Alkaline mixtures (e.g., potassium acetate, potassium citrate, or potassium carbonate) (to cause saponification)

Water and other liquids cannot be used on Class B/K fires because they would vaporize, causing an explosion and spreading the burning liquids all over the area. Water cannot be used on Class C fires because of the potential for electrocution. Oxygen suppression cannot be used on metal fires because burning metal produces its own oxygen.

Fire Detection Systems

Properly protecting a facility from fire requires installing an automated detection and suppression system. There are many types of fire detection systems. *Fixed-temperature detection* systems trigger suppression when a specific temperature is reached. This is the most common type of detector and is present in most office buildings. The potentially visible sprinkler head serves as both the detection and release mechanism. The trigger is usually a metal or plastic component that is in the sprinkler head and melts at a specific temperature. There is also a version with a small glass vial containing chemicals that vaporize to over-pressurize and shatter the container at a specific temperature. This system is inexpensive and reliable, even over long time periods.

Rate-of-rise detection systems trigger suppression when the speed at which the temperature changes reaches a specific level. These are often digital temperature measuring devices, which can be fooled by HVAC heating during winter months and thus are not widely deployed.

Flame-actuated systems trigger suppression based on the infrared energy of flames. This mechanism is fast and reliable but often fairly expensive. Thus, it is often only used in high-risk environments.

Smoke-actuated systems use photoelectric or radioactive ionization sensors as triggers. Either method monitors for light or radiation obstruction or reduction across an air gap caused by

particles in the air. It is intended to be triggered by smoke, but dust and steam can sometimes trigger the alarm. The radioactive ionization-based smoke detectors use americium as a source of alpha particles and a Geiger counter to detect the rate of these particles' transmission across the air gap. This element produces such low levels of radiation that a layer of dead skin cells is sufficient to block its transmission.

Incipient smoke detection systems, also known as aspirating sensors, are able to detect the chemicals typically associated with the very early stages of combustion before a fire is otherwise detectable via other means. These devices are even more costly than flame-actuated sensors and are also only used in high-risk or critical environments.

To be effective, fire detectors need to be placed strategically. Don't forget to place them inside dropped ceilings and raised floors, in server rooms, in private offices and public areas, in HVAC vents, in elevator shafts, in the basement, and so on.

Once a fire-detection device notices the presence of a fire, it typically will trigger the fire alarm. Most fire alarms are loud, piercing beeps or sirens paired with brightly flashing lights. A fire alarm is intended to be obvious, startling, and attention-grabbing. There is usually no mistaking a fire alarm or “not noticing” that it went off. Once a fire alarm occurs, all personnel should follow their safety training and begin to exit the building.

Most fire-detection systems can be linked to fire response service notification mechanisms. When suppression is triggered, such linked systems will contact the local fire response team and request aid using an automated message or alarm.

As for fire suppression mechanisms, they can be based on a water or gas system. Water is common in human-friendly environments, whereas gaseous systems are more appropriate where personnel typically do not reside and generally in non-human-compatible areas, such as engine compartments or equipment panels.

Water Suppression Systems

There are four main types of water suppression systems:

- A *wet pipe system* (also known as a *closed head system*) is always full of water. Water discharges immediately when suppression is triggered.
- A *dry pipe system* contains a compressed inert gas. Once suppression is triggered, the inert gas is released, opening a water valve that causes the pipes to fill and discharge water into the environment moments later.
- A *preaction system* is a variation of the dry pipe system that uses a two-stage detection and release mechanism. The system exists as a dry pipe until the initial stages of a fire (smoke, heat, and so on) are detected, and then the pipes are allowed to fill with water (Stage 1). The water is released only after the sprinkler head activation triggers are triggered by sufficient heat (Stage 2). If the fire is quenched before sprinklers are triggered, pipes can be manually emptied and reset. This also allows manual intervention (typically via a button mounted on a wall) to stop the release of water before sprinkler release occurs.
- A *deluge system* is a system that uses larger pipes and delivers a significantly larger volume of water compared to a wet pipe system. Also, when one sprinkler head opens, they all open to deluge the area fully with suppressant. Deluge systems are inappropriate for environments that contain electronics and computers.

Preaction systems are the most appropriate water-based system for environments that house both computers and humans together because they provide the opportunity to prevent the release of water in the event of a false alarm or false initial trigger.

The most common cause of failure for a water-based system is human error, such as turning off a water source when a fire occurs or triggering water release when there is no fire.

Gas Discharge Systems

Gas discharge systems use compressed gas to extinguish fire effectively. However, gas discharge systems should not be used in environments in which people are located. Gas discharge systems usually remove the oxygen from the air, thus making them hazardous to personnel. They employ a pressurized gaseous suppression medium, such as carbon dioxide (CO_2), halon, or *FM-200* (a halon replacement, although it too is already slated to be phased out). Benefits of gas-based fire suppression include causing the least damage to computer systems, extinguishing the fire quickly by removing oxygen, and being more effective and faster than a water-based system.

CO_2 is an effective fire suppressant, but it poses a risk to people. If CO_2 leaks into an enclosed space, it can cause asphyxiation at only a 7.5 percent concentration. Fire suppressant use of CO_2 is often at 34 percent or higher concentration. CO_2 is naturally colorless, odorless, and tasteless, so extreme care must be used when deploying a CO_2 system. There are some additives available to induce an odor. Due to its risks, CO_2 should be implemented only in special circumstances where personnel will not be present and a water-based system is inappropriate, such as engine compartments, generator rooms, around flammable liquids, and large industrial equipment. CO_2 is able to reduce temperatures as well as keep oxygen away from combustion locations.

Halon is an effective fire suppression compound (it starves a fire of oxygen by disrupting the chemical reaction of combustion), but it degrades into toxic gases at 900 degrees Fahrenheit. Also, it is not environmentally friendly (it is an ozone-depleting

substance). The 1989 Montreal Protocol (an international agreement) initiated the termination of manufacturing of ozone-depleting substances, including halon. In 1994, the EPA banned the manufacture of halon in the United States and banned importing halon into the country. However, according to the Montreal Protocol, you can obtain halon by contacting a halon recycling facility. The EPA seeks to exhaust existing stocks of halon to take this substance out of circulation, although there are still significant domestic stockpiles of halon.

Due to halon's issues, it is often replaced by a more ecologically friendly and less toxic medium. There are dozens of EPA-approved substitutes for halon. You can also replace halon substitutes with low-pressure water mists, but such systems are usually not employed in computer rooms or electrical equipment storage facilities. A low-pressure water mist is a vapor cloud used to reduce the temperature in an area quickly.

Damage

Addressing fire detection and suppression includes dealing with possible contamination and damage caused by a fire. The destructive elements of a fire include smoke and heat, but they also include the suppression media, such as water or soda acid. Smoke and soot are damaging to storage devices and many computer components. Heat can damage any electronic or computer component. For example, temperatures of 100 degrees Fahrenheit can damage storage tapes, 175 degrees can damage computer hardware (CPU and RAM), and 350 degrees can damage paper products (through warping and discoloration).

Suppression media can cause short circuits, initiate corrosion, or otherwise render equipment useless. All these issues must be addressed when designing a fire response system. Even a small fire might trigger the Incident Response Plan (IRP), Business Continuity Plan (BCP), or Disaster Recovery Plan (DRP).

Don't forget that in the event of a fire, in addition to damage caused by the flames and your chosen suppression medium, fire department members may inflict damage using water hoses and axes while searching for people to rescue and hot spots to extinguish.

Implement and Manage Physical Security

Many types of physical access control mechanisms can be deployed in an environment to control, monitor, and manage access to a facility. These range from deterrents to detection mechanisms. The various sections, divisions, or areas within a site or facility should be clearly designated as public, private, or restricted. Each of these areas requires unique and focused physical access controls, monitoring, and prevention mechanisms. The following sections discuss many such mechanisms that may be used to separate, isolate, and control access to various areas of a site, including perimeter and internal security.

Signage or signs can be used to declare areas off-limits to those who are not authorized, indicate that security cameras are in use, indicate entrances and exits, and disclose safety warnings. Signs are useful in deterring minor criminal activity, establishing a basis for recording events, and guiding people into compliance or adherence with rules or safety precautions. Signs are usually physical displays with words or images, but digital signs and warning banners should also be implemented on both local and remote connections.

If not mandated by regulations, a self-imposed schedule of control testing should be implemented for door locks, fences, gates, person traps, turnstiles, video cameras, and all other physical security controls.

Perimeter Security Controls

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

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

Fences, Gates, Turnstiles, and Person Traps

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

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

An advanced form of fencing is known as a *perimeter intrusion detection and assessment system (PIDAS)*. A PIDAS is a fence system that has two or three fences used in concert to optimize security. PIDAS fencing is often present around military locations

and prisons. Typically, a PIDAS fence has one main tall fence that may be 8 to 20 feet tall. The main fence may be electrified, may have barbed wire/razor wire elements, and/or can include touch detection technologies. This main fence is then surrounded by an outside fence, which may only be 4 to 6 feet tall. The purpose of this outer fence is to keep animals and casual trespassers from accessing the main fence. This reduces the *nuisance alarm rate (NAR)* or false positives from animals or foliage on interior fences. Additional fences can be located between the main fence and the exterior fence. These additional fences may be electrified or use barbed/razor wire. The space between the fences can serve as a corridor for guard patrols or wandering guard dogs. These corridors are kept free of vegetation.

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

A *turnstile* (see Figure 10.5) is a form of gate that prevents more than one person at a time from gaining entry and often restricts movement in one direction. It is used to gain entry but not to exit, or vice versa. A turnstile is basically the fencing equivalent of a secured revolving door. A turnstile can be designed to turn freely to allow easy egress. An ingress turnstile can be implemented with a locking mechanism that requires personnel to provide a code, combination, or credential before it will allow a single person to enter the secured area. A turnstile can be used as a personnel flow control device to limit the direction of travel and the speed of access (i.e., only one person can pass at a time after valid authentication).

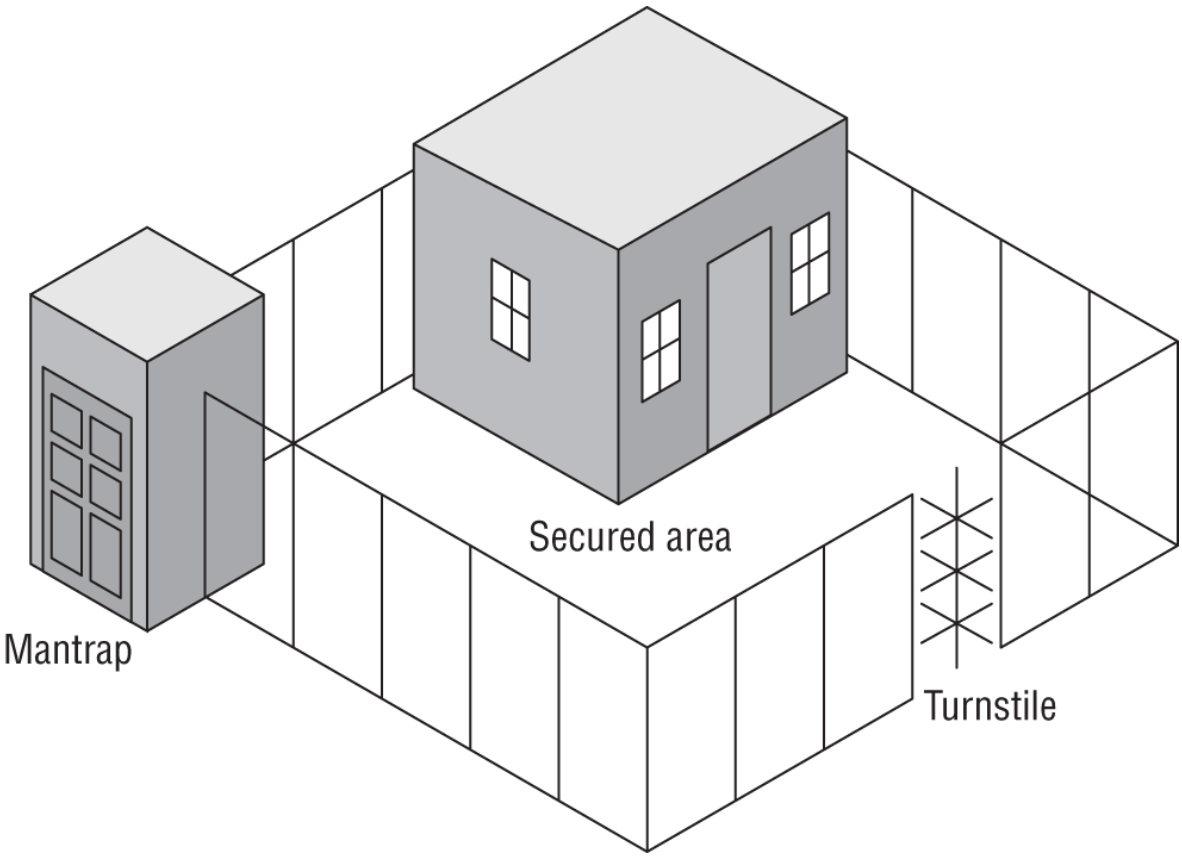

FIGURE 10.5 A secure physical boundary with a person trap and a turnstile

A person trap (also known as a man trap or an *access control vestibule*) is a double set of doors (also shown in Figure 10.5) that is often protected by a guard or some other physical layout that prevents piggybacking and can trap individuals at the discretion of security personnel. The purpose of a person trap is to immobilize a subject until their identity and authentication authority are verified. If a subject is authorized for entry, the inner door opens, allowing entry into the facility or onto the premises. If a subject is not authorized, both doors remain closed and locked until an escort (typically a guard or a police officer) arrives to escort the subject off the property or arrest the subject for trespassing (this is known as a delay feature). Often, a person trap includes a scale to prevent piggybacking or tailgating. Person traps can be used to control entrance into a facility or entrance within a facility to a higher secured area, such as a data center or an SCIF.

Another key element of physical security, especially for data centers, government facilities, and highly secure organizations, is *security bollards*, which prevent vehicles from ramming access points and entrances. These can be permanently fixed in place or automatically rise from their installed base at a fixed time or an alert. They are often disguised as planters or other architectural elements. See the previous discussion of CPTED in the "Facility Design" section.

Barricades, in addition to fencing, are used to control both foot traffic and vehicles. K-rails (often seen during road construction), large planters, zigzag queues, bollards, and tire shredders are all examples of barricades. When used properly, they can control crowds and prevent vehicles from being used to cause damage to your building. Long, straight, and unobstructed vehicle paths should be avoided to prevent the buildup of excessive speed. If generators and fuel storage are present, additional layers of barricade protection may be necessary to prevent tampering or destruction.

Lighting

Lighting is the most commonly used form of perimeter security control, providing the security benefit of deterrence. The primary purpose of lighting is to discourage casual intruders, trespassers, prowlers, or would-be thieves who would rather perform their misdeeds, such as vandalism, theft, and loitering, in the dark. Both interior and exterior lighting should be implemented for security, especially related to parking areas, walkways, and entrances. Exterior lighting should generally be on from dusk until dawn. Interior lighting may be always on, switched manually, or triggered on demand, possibly via motion. Emergency lighting should be implemented in key areas (such as exits and escape routes) and triggered with the loss of power or along with a fire alarm. Lighting is often claimed to be the most commonly deployed physical security mechanism. However, lighting is only a deterrent and not a strong deterrent. It should not be used as the primary or sole protection mechanism except in areas with a low threat level. Your entire site, inside and out,

should be well lit. This provides for easy identification of personnel and makes it easier to notice intrusions.

Lighting should not necessarily be used to illuminate the positions of guards, dogs, patrol posts, or other similar security elements. However, these can be illuminated if knowledge of their presence is to be used as a deterrent. Lighting should be combined with security guards, guard dogs, security cameras, or some other form of intrusion detection or surveillance mechanism. Lighting must not cause a nuisance or problem for nearby residents, roads, railways, airports, and so on. It should also never cause glare or reflective distraction to guards, dogs, and monitoring equipment, which could otherwise aid attackers during break-in attempts. Strong lights used to illuminate a building located on a fence line pointing inward can function as a means to hide intruders. Just think of standing in the dark with someone pointing a flashlight at you—you will be unable to see the other person because the light pointing toward you overpowers your vision.

It is generally accepted as a de facto standard that lighting used for perimeter protection should illuminate critical areas with at least 2 foot-candles of power (which is approximately 2 lumens, or 20 lux). Another common issue for the use of lighting is the placement of the lights. Standards seem to indicate that light poles should be placed the same distance apart as the diameter of the illuminated area created by illumination elements. Thus, if a lighted area is 40 feet in diameter, poles should be 40 feet apart (although it seems to us that placing the poles about 10–20 percent closer is a better option to ensure overlapping of the illuminated areas). This light pole positioning allows for the intersection of lighted areas on the ground, thus preventing an intruder from gaining access under the cover of darkness.

Security Guards and Guard Dogs

All physical security controls, whether static deterrents or active detection and surveillance mechanisms, ultimately rely on personnel to intervene and prevent actual intrusions and attacks. *Security guards* exist to fulfill this need. Guards can be posted

around a perimeter or inside to monitor access points or watch detection and surveillance monitors. The real benefit of guards is that they are able to adapt and react to various conditions or situations. Guards can learn and recognize attack and intrusion activities and patterns, can adjust to a changing environment, and can make decisions and judgment calls. Security guards are often an appropriate security control when immediate situation handling and decision-making on-site is necessary.

Guards should perform patrols both internally and externally to look for security violations, unauthorized entities, or other abnormalities throughout the facility and campus grounds. Patrols should be frequent, but at random intervals. This prevents an intruder from observing a pattern of patrols and then timing their break-in accordingly.

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

Even if a guard is initially reliable, guards are subject to physical injury and illness, take vacations, can become distracted, are vulnerable to social engineering, and may become unemployable because of substance abuse. In addition, security guards usually offer protection only up to the point at which their life is endangered. Additionally, security guards are usually unaware of the scope of the operations within a facility and are, therefore, not thoroughly equipped to know how to respond to every situation. Though this is considered a disadvantage, the lack of knowledge of the scope of the operations within a facility can also be considered an advantage, because this supports the confidentiality of those operations and thus helps reduce the possibility that a security guard will be involved in the disclosure of confidential information. Finally, security guards are

expensive, whether they are employees or are provided by a third-party contractor.

Guard dogs can be an alternative to security guards. They can often be deployed as a perimeter security control. As a detection and deterrent, dogs are extremely effective. However, dogs are costly, require a high level of maintenance (i.e., housing, feeding, health care, training, etc.), and impose serious insurance and liability requirements.

Robot sentries can be used to patrol an area automatically to look for anything out of place. Robot sentries often use facial recognition to identify authorized individuals and potentially identify intruders. Robot sentries can be on wheels or a flying drone (aka uncrewed aerial vehicle [UAV]).

Internal Security Controls

A mechanism to handle visitors is required if a facility is designed with restricted areas to control physical security. Often, an escort is assigned to visitors, and their access and activities are monitored closely. Failing to track the actions of outsiders when they are allowed into a protected area can result in malicious activity against the most protected assets. Visitor control can also benefit from the use of keys, combination locks, badges, motion detectors, intrusion alarms, and more.

Reception can be used as a choke point to block access to unauthorized visitors. The reception area should be segregated from the security areas with locked doors and monitored by security cameras. If a visitor is authorized, then an escort can be assigned to accompany them around the facility. If a valid worker arrives, the receptionist may be able to "buzz" the door open for them. Any unauthorized visitors can be asked to leave, security guards can be brought to bear, or police can be called.

Visitor logs are a manual or automated list of nonemployee entries or access to a facility or location. Employee logs may also be useful for access tracking and verification. Logs of physical access should be maintained. These can be created automatically through the use of smartcards or manually by a security guard.

The physical access logs establish context for the interpretation of logical logs. Logs are helpful in an emergency to determine whether everyone has escaped a building safely.

Keys and Combination Locks

Locks keep closed doors closed. They are designed and deployed to prevent access to everyone without proper authorization. A *lock* is a crude form of an identification and authorization mechanism. If you possess the correct key or combination, you are considered authorized and permitted entry. Key-based locks are the most common and inexpensive forms of physical access control devices. These are often known as *preset, deadbolt*, or conventional locks. These types of locks are subject to *lock picking*, which is often categorized under a class of lock mechanism attacks called *shimming*. Many conventional locks are also vulnerable to an attack known as bumping. *Bumping* is accomplished using a special bump key that when properly tapped or bumped causes the lock pins to jump and allows the cylinder to turn.

Programmable or combination locks offer a broader range of control than preset locks. Some programmable locks can be configured with multiple valid access combinations or may include digital or electronic controls employing keypads, smartcards, or cipher devices. For instance, an *electronic access control (EAC) lock* incorporates three elements: an electromagnet to keep the door closed, a credential reader to authenticate subjects and deactivate the electromagnet, and a sensor to reengage the electromagnet when the door is closed. An EAC can monitor the amount of time that a door stays open to trigger a warning buzzer if a door stays open for longer than 5 seconds and trigger an intrusion alarm if the door stays open for longer than 10 seconds (times are examples, not prescriptions).

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

Environmental Issues and Life Safety

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

Part of maintaining personnel safety is maintaining a facility's basic environment. People can survive for short periods without water, food, power, and air conditioning. But in some cases, the loss of these elements can have disastrous results or be symptoms of more immediate and dangerous problems. Flooding, fires, release of toxic materials, natural disasters, and human-made disasters all threaten human life as well as the stability of a facility. Physical security procedures should focus on protecting human life, restoring the environment's safety, and restoring the utilities necessary for the IT infrastructure to function.

People should always be your top priority. Only after personnel are safe can you consider addressing business continuity. Many organizations adopt *occupant emergency plans (OEPs)* to guide and assist with sustaining personnel safety after a disaster. The OEP guides how to minimize threats to life, prevent injury, manage duress, handle travel, provide safety monitoring, and protect property from damage due to a destructive physical event. The OEP does not address IT issues or business continuity, just personnel and general property. The business continuity plan (BCP) and disaster recovery plan (DRP) address IT and business continuity and recovery issues.

Regulatory Requirements

Every organization operates within a certain industry and jurisdiction. Both of these entities (and possibly additional ones) impose legal requirements, restrictions, and regulations on the practices of organizations that fall within their realm. These legal requirements can apply to the licensed use of software, hiring

restrictions, handling of sensitive materials, and compliance with safety regulations.

Complying with all applicable legal requirements is a key part of sustaining security. The legal requirements for an industry and a country (and often also a state and city) must be considered a baseline or foundation on which the remainder of the security infrastructure is built.

Key Performance Indicators of Physical Security

Key performance indicators (KPIs) of physical security should be determined, monitored, recorded, and evaluated. KPIs are metrics or measurements of the operation or failure of various aspects of physical security. The goal of using KPIs is to assess the effectiveness of security efforts. Only with such information can management make informed decisions on altering existing security operations to achieve a higher level of effective security protection. Keep in mind that the overall goal of security is to reduce risk so that the organization's objectives can be achieved cost-effectively.

Here are common and potential examples of physical security KPIs:

- Number of successful intrusions
- Number of successful crimes
- Number of successful incidents
- Number of successful disruptions
- Number of unsuccessful intrusions
- Number of unsuccessful crimes
- Number of unsuccessful incidents
- Number of unsuccessful disruptions
- Time to detect incidents
- Time to assess incidents

- Time to respond to incidents
- Time to recover from incidents
- Time to restore normal conditions after an incident
- Level of organizational impact of incidents
- Number of false positives (i.e., false detection alerts/alarms)

A baseline should be established for each KPI, and a record of each measurement should be maintained. This historical record and baseline are necessary to perform trend analysis and gain an understanding of the performance of the physical security mechanisms. Automatically collected KPIs are often preferred, since they will be recorded reliably. Manual KPI measurements are often more important, but they require attention and focus to collect. Each incident response operation (even if a BCP and DRP level issue), should conclude with a lessons learned phase where/when any additional KPI-related information is gathered or determined and recorded. With reliable KPI assessment, organizations can identify deficiencies, assess improvements, evaluate response measures, and perform return on security investment (ROSI) and cost/benefit analysis for physical security controls.

Summary

In all circumstances and under all conditions, the most important goal of security is protecting people.

Several elements are involved in implementing and maintaining physical security. One core element is selecting or designing the facility to house your IT infrastructure and the operations of your organization. You must start with a plan that outlines the security needs for your organization and develops through a process known as critical path analysis. Additional elements of a secure facility plan are evaluating site selection and visibility requirements and considering facility design elements such as Crime Prevention Through Environmental Design (CPTED).

The security controls implemented to manage physical security can be divided into three groups: administrative (management, managerial, or procedural), technical (logical), and physical. Administrative physical security controls include facility construction and selection, site management, building design, personnel controls, awareness training, and emergency response and procedures. Technical physical security controls include building access controls; intrusion detection; alarms; security cameras; monitoring; heating, ventilation, and air-conditioning (HVAC) power supplies; and fire detection and suppression. Physical controls for physical security include fencing, lighting, locks, construction materials, a person trap, guard dogs, and security guards.

Wiring closets and server rooms are important infrastructure elements that require protection. They often house core networking devices and other sensitive equipment. Protections include adequate locks, smartcards for authentication, proximity devices and readers intrusion detection systems, cameras, surveillance, access control, and regular physical inspections.

An important aspect of physical access control and maintaining a facility's security is protecting the environment's basic elements; this may include the use of media storage facilities, evidence storage, and work area restrictions. Providing clean power sources, minimizing interference, and managing the environment are also important.

Fire detection and suppression must not be overlooked. In addition to protecting people, fire detection and suppression are designed to keep damage caused by fire, smoke, heat, and suppression materials to a minimum, especially regarding the IT infrastructure.

Additional physical security mechanisms to implement and manage include perimeter breach detection, fences, gates, turnstiles, person traps, lighting, security guards, guard dogs, locks, badges, protected cable distribution, motion detectors, intrusion alarms, and secondary verification mechanisms. It is also essential to evaluate regulatory compliance and track KPIs.

Study Essentials

Understand why there is no security without physical security. Without control over the physical environment, no amount of administrative or technical/logical access controls can provide adequate security. If a malicious person can gain physical access to your facility or equipment, they can do just about anything they want, from destruction to disclosure and alteration.

Understand a security facility plan. A secure facility plan outlines your organization's security needs and emphasizes methods or mechanisms to provide security. Such a plan is developed through risk assessment and critical path analysis.

Know about technology convergence. Technology convergence is the tendency for various technologies, solutions, utilities, and systems to evolve and merge over time. Though this can result in improved efficiency and cost savings in some instances, it can also represent a single point of failure and become a more valuable target for malicious actors and intruders.

Understand site selection. Site selection should be based on the security needs of the organization. Cost, location, and size are important, but addressing the requirements of security should always take precedence. The key elements in selecting a site are visibility, composition of the surrounding area, and accessibility.

Know the key elements in designing a facility for construction. A key element in designing a facility for construction is understanding the level of security needed by your organization and planning for it before construction begins.

Know the functional order of controls. These are deter, deny, detect, delay, determine, and decide.

Understand equipment failure. No matter the quality of the equipment your organization chooses to purchase and install, eventually, it will fail. Preparing for equipment failure may include purchasing replacement parts, storing equipment, or having an SLA with a vendor.

Know how to design and configure secure work areas. There should not be equal access to all locations within a facility. Areas that contain assets of higher value or importance should have restricted access. Valuable and confidential assets should be located in the heart or center of protection provided by a facility.

Understand the security concerns of a wiring closet. A wiring closet is where the networking cables for a whole building or just a floor are connected to other essential equipment, such as patch panels, switches, routers, LAN extenders, and backbone channels. Most of the wiring closet security focuses on preventing unauthorized access. If an unauthorized intruder gains access to the area, they may be able to steal equipment, pull or cut cables, or even plant a listening device.

Know about proximity devices and readers. A proximity device can be a passive device, a field-powered device, or a transponder. When it passes near a proximity reader, the reader device is able to determine who the bearer is and whether they have authorized access.

Understand intrusion detection systems. Intrusion detection systems (IDSs) or burglar alarms are automated or manual systems designed to detect an attempted intrusion, breach, or attack; the use of an unauthorized entry point; or the occurrence of some specific event at an unauthorized or abnormal time.

Know about cameras. Video surveillance, video monitoring, closed-circuit television (CCTV), and security cameras are all means to deter unwanted activity and create a digital record of the occurrence of events. Cameras can be overt or hidden; can record locally or to a cloud storage service; may offer pan, tilt, and zoom; may operate in visible or infrared light; may be triggered by movement; and may support time-lapse recording, tracking, facial recognition, gait analysis, object detection, or infrared or color-filtered recording.

Understand security needs for media storage. Media storage facilities should be designed to store blank media, reusable media, and installation media securely. The concerns

include theft, corruption, and data remnant recovery. Media storage facility protections include using locked cabinets or safes, using a media librarian/custodian, implementing a check-in/checkout process, and using media sanitization.

Understand the concerns of evidence storage. Evidence storage is used to retain logs, drive images, virtual machine snapshots, and other datasets for recovery, internal investigations, and forensic investigations. Protections include dedicated/isolated storage facilities, offline storage, activity tracking, hash management, access restrictions, and encryption.

Know the common threats to physical access controls. No matter what form of physical access control is used, a security guard or other monitoring system must be deployed to prevent abuse, impersonation, masquerading, tailgating, and piggybacking.

Understand how to control your environment. In addition to power considerations, maintaining the environment involves control over the HVAC mechanisms. Rooms containing primarily computers should be kept at 59 to 89.6 degrees Fahrenheit (15 to 32 degrees Celsius). Humidity in a computer room should be maintained between 20 and 80 percent. Too much humidity can cause corrosion. Too little humidity causes static electricity.

Understand the need to manage water leakage and flooding. Your environmental safety policy and procedures should address water leakage and flooding. Water and electricity don't mix. Locate server rooms and critical computer equipment away from any water source or transport pipes whenever possible.

Understand the importance of fire detection and suppression. Protecting personnel from harm should always be the most important goal of any security or protection system. In addition to protecting people, fire detection and suppression are designed to keep damage caused by fire, smoke, heat, and suppression materials to a minimum, especially in regard to the IT infrastructure.

Know about physical perimeter security controls. Controlled access to a facility can be accomplished using fences, gates, turnstiles, person traps, bollards, and barricades.

Know about security guards and guard dogs. Guards can be posted around a perimeter or inside to monitor access points or watch detection and surveillance monitors. Guards are able to adapt and react to various conditions or situations and can learn and recognize attack and intrusion activities and patterns, adjust to a changing environment, and make decisions and judgment calls. An alternative to security guards, guard dogs can often be deployed as a perimeter security control and are an extremely effective detection and deterrent.

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

Understand internal security controls. There are many physical security mechanisms for internal control, including locks, badges, protective distribution systems (PDSs), motion detectors, intrusion alarms, and secondary verification mechanisms.

Know about KPIs of physical security. Physical security's key performance indicators (KPIs) should be determined, monitored, recorded, and evaluated. KPIs are metrics or measurements of the operation or failure of various aspects of physical security.

Written Lab

1. What kind of device helps to define an organization's perimeter and also serves to deter casual trespassing?
2. What is the problem with halon-based fire suppression technology?