Processor Security Extensions

TEEs need hardware support, which all the major chip manufacturers provide in their chipsets. Security is baked into the chips of most modern microprocessors. These CPU packages become a security perimeter outside of which all data and code can exist in encrypted form. Before encrypted data or code can cross into the secure perimeter, it can be decrypted and/or checked for integrity. Even once allowed inside, data and code are restricted by special controls that ensure what may be done with or to them. For all this to work, however, we need to enable the features through special instructions.

Processor security extensions are instructions that provide these security features in the CPU and can be used to support a TEE. They can, for example, enable programmers to designate special regions in memory as being encrypted and private for a given process. These regions are dynamically decrypted by the CPU while in use, which means any unauthorized process, including the OS or a hypervisor, is unable to access the plaintext stored in them. This feature is one of the building blocks of TEEs, which enables trusted applications to have their own protected memory.

Atomic Execution

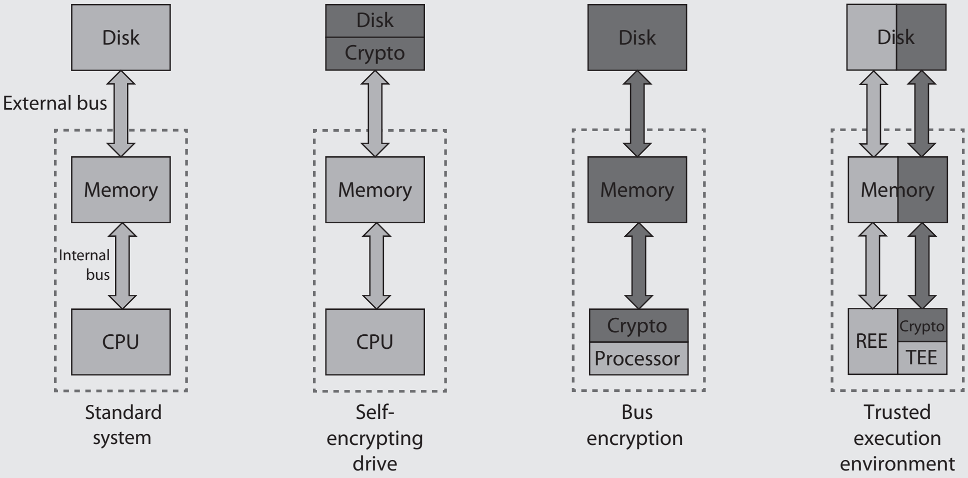
Atomic execution is an approach to controlling the manner in which certain sections of a program run so that they cannot be interrupted between the start and end of a section. This prevents other processes from interfering with resources being used by the protected process. To enable this, the programmer designates a section of code as atomic by placing a lock around it. The compiler then leverages OS libraries that, in turn, invoke hardware protections during execution of that locked code segment. The catch is that if you do this too often, you will see some dramatic performance degradation in a modern multithreaded OS. You want to use atomic execution as little as possible to protect critical resources and tasks.

Atomic execution protects against a class of attacks called *time-of-check to time-of-use (TOC/TOU)*. This type of attack exploits the dependency on the timing of events that take place in a multitasking OS. When running a program, an OS must carry out instruction 1, then instruction 2, then instruction 3, and so on. This is how programs are normally written. If an attacker can get in between instructions 2 and 3 and manipulate something, she can control the result of these activities. Suppose instruction 1 verifies that a user is authorized to read an unimportant file that is passed as a link, say, a help file. Instruction 2 then opens the file pointed to by the link, and instruction 3 closes it after it's been read by the user. If an attacker can interrupt this flow of execution after instruction 1, change the link to point to a sensitive document, and then allow instruction 2 to execute, the attacker will be able to read the sensitive file even though she isn't authorized to do so. By enforcing atomic execution of instructions 1 and 2 together, we would protect against TOC/TOU attacks.

NOTE This type of attack is also referred to as an asynchronous attack. *Asynchronous* describes a process in which the timing of each step may vary. The attacker gets in between these steps and modifies something.

Putting It All Together: Where Can Data Be Encrypted?

Data in a computer system can exist in three different places: in the processor, in memory, and in secondary storage such as a disk drive. Standard systems do not encrypt data in any of these three places by default. You can opt to use FED, such as a self-encrypting drive, to encrypt the data in secondary storage, but that leaves it exposed everywhere else in the system, including the external bus. The third option is to use bus encryption, which requires a cryptoprocessor that is (relatively) expensive and underpowered. You are unlikely to want this unless you *really* have to protect the data in situations where you assume the adversary will be able to hack your hardware. Finally, the most flexible (and common) balance of protection, performance, and cost is the use of TEEs that can coexist with untrusted applications. Only the data within the TEE receives the full encryption treatment outside the CPU, leaving everything else to run on regular processor cores.



Chapter Review

One of the keys to providing the best security possible is to have a baseline understanding of adversaries that may target the organization, what their capabilities are, and what motivates them. We saw multiple ways to do that in this chapter, of which the MITRE ATT&CK framework is probably the one you want to dig into on your own. It seems like many professionals and organizations alike are converging on it as the *lingua franca* by which to describe adversarial behaviors.

A sound approach to defeating these threat actors is to apply the fundamental principles of secure design, of which we covered the 11 that ISC^2 stresses in the CISSP Certification

Exam Outline. There are other principles that you may be tracking, but these are the 11 you'll need to know for the exam. Likewise, the security models we discussed, which bring extra rigor to the study of security, are sure to make an appearance in the exam. Pay particular attention to Biba and Bell-LaPadula. Together, these principles and models provide a solid foundation on which to select controls based upon systems security requirements and build a solid security architecture.

Quick Review

- Threat modeling is the process of describing probable adverse effects on our assets caused by specific threat sources.
- An attack tree is a graph showing how individual actions by attackers can be chained together to achieve their goals.
- STRIDE is a threat modeling framework developed by Microsoft that evaluates a system's design using flow diagrams, system entities, and events related to a system.
- The Lockheed Martin Cyber Kill Chain identifies seven stages of cyberattacks.
- The MITRE ATT&CK framework is a comprehensive matrix of tactics and techniques used to model cyberattacks.
- Defense in depth is the coordinated use of multiple security controls in a layered approach.
- Zero trust is a model in which every entity is considered hostile until proven otherwise, and even that trust is limited.
- Trust but verify is the principle that, even when an entity and its behaviors are trusted, we should double-check both.
- Shared responsibility refers to the situation in which a service provider is responsible for certain security controls, while the customer is responsible for others.
- Separation of duties divides important functions among multiple individuals to ensure that no one person has the ability to intentionally or accidentally cause serious losses to the organization.
- Least privilege states that people are granted exactly the access and authority that they require to do their jobs, and nothing more.
- The need-to-know principle, which is similar to the least-privilege principle, is based on the concept that individuals should be given access only to the information they absolutely require in order to perform their job duties.
- The "keep it simple" principle drives us to make everything as simple as possible and periodically check things to ensure we are not adding unnecessary complexity.
- The principle of secure defaults means that every system starts off in a state where security trumps user friendliness and functionality.

- The principle of failing securely states that, in the event of an error, information systems ought to be designed to behave in a predictable and noncompromising manner.
- The principle of privacy by design states that the best way to ensure privacy of user data is to incorporate data protection as an integral part of the design of an information system, not as an afterthought or later-stage feature.
- The Bell-LaPadula model enforces the confidentiality aspects of access control.
- The Biba model is a security model that addresses the integrity of data within a system but is not concerned with security levels and confidentiality.
- The Brewer and Nash model, also called the Chinese Wall model, states that a subject can write to an object if, and only if, the subject cannot read another object that is in a different dataset.
- A Trusted Platform Module (TPM) is dedicated to carrying out security functions involving the storage of cryptographic keys and digital certificates, symmetric and asymmetric encryption, and hashing.
- A hardware security module (HSM) is a removable expansion card or external device that can generate, store, and manage cryptographic keys to improve encryption/decryption performance of the system into which it is installed.
- A self-encrypting drive (SED) provides full disk encryption (FDE) through a cryptographic module that is integrated with the storage media into one package.
- Data in SEDs is encrypted using symmetric key cryptography.
- Bus encryption systems use TPMs to encrypt data and instructions prior to being put on the internal bus, which means they are also encrypted everywhere else except when data is being processed.
- A trusted execution environment (TEE), or a secure enclave, is a software environment in which special applications and resources (such as files) have undergone rigorous checks to ensure that they are trustworthy and remain protected.
- Processor security extensions are instructions that provide additional security features in the CPU and can be used to support a TEE.
- Atomic execution is an approach to controlling the manner in which certain sections of a program run so that they cannot be interrupted between the start and end of the section.

Questions

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

1. Developed by Microsoft, which threat-modeling technique is suitable for application to logical and physical systems alike?

A. Attack trees

B. STRIDE

C. The MITRE ATT&CK framework

D. The Cyber Kill Chain

2. Which threat modeling framework provides detailed procedures followed by specific cyberthreat actors?

A. Attack trees

B. STRIDE

C. The MITRE ATT&CK framework

D. The Cyber Kill Chain

3. Which of the following security models is concerned with the confidentiality and not the integrity of information?

A. Biba

B. Bell-LaPadula

C. Brewer and Nash

D. Clark-Wilson

4. Which of the following security models is concerned with the integrity and not the confidentiality of information?

A. Biba

B. Bell-LaPadula

C. Graham-Denning

D. Brewer and Nash

5. Where is the data encrypted in a self-encrypting drive system?

A. On the disk drive

B. In memory

C. On the bus

D. All of the above

6. Where is the data encrypted in a bus encryption system?

A. On the disk drive

B. In memory

C. On the bus

D. All of the above

7. What is the difference between a Trusted Platform Module (TPM) and a hardware security module (HSM)?
   A. An HSM is typically on the motherboard and a TPM is an external device.
   B. Only an HSM can store multiple digital certificates.
   C. There is no difference, as both terms refer to the same type of device.
   D. A TPM is typically on the motherboard and an HSM is an external device.

8. Which of the following is *not* a required feature in a TPM?
   A. Hashing
   B. Certificate revocation
   C. Certificate storage
   D. Encryption

9. Which of the following is true about changing the password on a self-encrypting drive?
   A. It requires re-encryption of stored data.
   B. The new password is encrypted with the existing secret key.
   C. It has no effect on the encrypted data.
   D. It causes a new secret key to be generated.

10. Which of these is true about processor security extensions?
   A. They are after-market additions by third parties.
   B. They must be disabled to establish trusted execution environments.
   C. They enable developers to encrypt memory associated with a process.
   D. Encryption is not normally one of their features.

Answers

1. **B.** STRIDE is a threat-modeling framework that evaluates a system's design using flow diagrams, system entities, and events related to a system.
2. **C.** The MITRE ATT&CK framework maps cyberthreat actor tactics to the techniques used for them and the detailed procedures used by specific threat actors during cyberattacks.
3. **B.** The Bell-LaPadula model enforces the confidentiality aspects of access control.
4. **A.** The Biba model is a security model that addresses the integrity of data within a system but is not concerned with security levels and confidentiality.
5. **A.** Self-encrypting drives include a hardware module that decrypts the data prior to putting it on the external bus, so the data is protected only on the drive itself.

6. **D.** In systems that incorporate bus encryption, the data is decrypted only on the cryptoprocessor. This means that the data is encrypted everywhere else on the system.
7. **D.** In general, TPMs are permanently mounted on the motherboard and used for hardware-based assurance and key storage, while HSMs are removable or altogether external and are used for both hardware accelerated cryptography and key storage.
8. **B.** Certificate revocation is not a required feature in a TPM. TPMs must provide storage of cryptographic keys and digital certificates, symmetric and asymmetric encryption, and hashing.
9. **C.** When you change the password on a self-encrypting drive, the existing secret key is retained but is encrypted with the new password. This means the encrypted data on the disk remains unaltered.
10. **C.** Processor security extensions are instructions that provide security features in the CPU and can be used to support a trusted execution environment. They can, for example, enable programmers to designate special regions in memory as being encrypted and private for a given process.

CHAPTER 10

Site and Facility Security

This chapter presents the following:

- Security principles of facility design
- Designing facility security controls

A building has at least two lives—the one imagined by its maker and the life it lives afterward—and they are never the same.

—Rem Koolhaas

We close out the third domain of the CISSP Common Body of Knowledge (CBK) by turning our attention to a topic to which many of us cybersecurity professionals don't pay enough attention: the security of our facilities and buildings. Most of us are focused on people and technology, but without a secure physical environment, all these efforts could be for naught. If adversaries can put their hands on our computers at will, it becomes much more difficult to keep them from also getting their hands on our information.

In this chapter, we take a good look at all that goes into securing the facilities that house our people, equipment, and information. Whether you get to build a site from scratch, have to choose an existing one, or are already occupying one, you should know and be able to apply the security principles we'll discuss here. We'll start off with the planning and design processes. Next, we'll examine how to apply the secure design principles (discussed in the previous chapter) to the overall design of a site or facility. We'll then explore how to refine that design by selecting specific controls that mitigate risks to tolerable levels. Although we don't explicitly cover it in this chapter (and just as with any other aspect of security), we must periodically review and test our plans and controls so that they remain effective and are continuously improved.

Site and Facility Design

The terms site and facility are oftentimes used interchangeably, and although the CISSP exam does not make a strong distinction between them, we should clarify what they each mean for purposes of this discussion. A *site* is a geographic area with fixed boundaries that typically contains at least one building and its supporting structures (e.g., a parking lot or electric substation). A *facility* is a building or a part of a building dedicated to a specific purpose, such as corporate headquarters or a data center. So, a site would include one or more facilities within it. Sometimes, an organization will have a facility inside someone else's site or even building, such as when an organization rents a group of connected offices (the facility) in a corporate plaza (the site).

EXAM TIP Don't worry about differentiating the terms site and facility for purposes of the exam.

Site planning, like almost anything else, starts with a good set of requirements. These depend upon the level of protection required for the various assets and the organization as a whole. This required level of protection, in turn, is determined by the risk management processes we discussed in Chapter 2, particularly the risk assessment. Physical security is a combination of structures, people, processes, procedures, technology, and equipment to protect resources. The design of a solid physical security program should be methodical and should weigh the objectives of the program and the available resources. Although every organization is different, the approach to constructing and maintaining a physical security program is the same. The organization must first define the vulnerabilities, threats, threat agents, and targets, which may be different than the ones we normally track in cybersecurity.

NOTE Remember that a vulnerability is a weakness and a threat is the event or mechanism that could actually exploit this identified vulnerability. The threat agent is the person or thing that initiates the threat against this identified vulnerability.

Security Principles

Let's take a moment to review the security principles covered in Chapter 9, which are equally applicable to designing secure networks and designing secure facilities. In the sections that follow, we briefly point out some examples of how these principles are applied in real organizations. We could provide many more examples, but the point is to show how the principles apply, not to be all-inclusive.

EXAM TIP You should be prepared to identify the application of the principles of secure design in a given scenario on the exam.

Threat Modeling

Securing anything, physical facilities included, should start with the question: securing it from what? Depending on the nature of our organizations and their environments, our concerns may range from petty thieves to terrorists. If we were to hold a brainstorming session, we could probably think of a very large set of potential threat actors carrying out an even larger set of harmful actions. It is helpful to narrow things down a bit by considering the most likely threat and then the most dangerous one too. For example, suppose your organization develops and sells productivity software. After a bit of threat modeling, you determine that your likeliest physical security threat is a fire accidentally started by employees overloading circuits (say, with portable space heaters) and your most dangerous physical threat is a competitor sneaking into your facility and copying your source code. So, you focus your attention on mitigating the risk that stems from those two threats, which allows you to apply your limited resources to the threats that matter most to you.

Things change, however, so threat modeling (just as the broader risk management) activities are ongoing. You should periodically reassess your threat models to ensure they remain accurate and up to date. Threat modeling includes not only the source of the risk (i.e., the threat actor) but also the manner in which that risk becomes manifest (i.e., the threat actor's specific actions). Continuing our earlier example, suppose you realize that your competitors are likelier to bribe an insider to exfiltrate the source code on a removable drive than to sneak into your facility and steal it themselves, so you update your threat models and ensure the right controls are in place. Or maybe your company's CEO makes a controversial statement and now your most dangerous adversary's course of action is that angry demonstrators will vandalize your facility. Either way, threat models need to be updated and security controls adjusted periodically.

Defense in Depth

Just like we think in terms of concentric layers of protection around our logical assets, we do the same with our physical ones. Whether your organization has an existing facility or is planning a new one, what is the outermost layer? It could be a fence or simply a row of concrete planters. Maybe your organization is located in a single building and the lobby is this first layer. Whatever the case, you want to balance the (oftentimes) competing needs of making the facility attractive and welcoming to legitimate visitors, while conveying the message that security is treated seriously.

Beyond the outer perimeter, you want to maintain the message that security is part of the design. Visitors should have to sign in and be escorted. All staff should wear badges that are different from badges issued to visitors. Cameras should be conspicuous throughout. "Restricted area" signs should be visible. To gain access to these restricted areas, staff should be required to badge in so that an audit record of who enters and leaves exists. We'll get into specific controls later in this chapter, but the point is that as one travels from the outside of the facility toward the most sensitive areas, security controls should be visible and increasingly tight.

Zero Trust

A threat that is frequently overlooked, even in some fairly secure environments, is that of the malicious insider. Whether that person is a member of the organization, a contractor, a partner, or even an impostor, it is not hard to come across news stories describing the damage malicious insiders have caused from within. Applying the principle of zero trust to securing our facilities means we need to be able to tell whether someone should be in a given part of our facility doing whatever it is they're doing. To this end, we could use badges with different colors or icons. For example, you could divide a site into black, gray, and gold sections and then label the rooms, hallways, and badges with the appropriate colors. If you come across someone with a badge that doesn't match the section in which they are located, you can approach or report them. Similarly, you could have icons on the badges that denote other authorizations. The following list gives you some ideas of the types of staff badge icons that are used in real organizations to display a staff member's restrictions, permissions, or status:

- Escort required
- Allowed to escort visitors
- Custodial staff
- Data center (or operations center, or C-suite) access
- Top secret security clearance
- Allowed to carry weapons

Another aspect of zero trust applied to physical security is the notion of "see something, say something." Staff members should be required by policy and trained to pay attention to suspicious situations and respond appropriately. Examples are challenging unbadged personnel in the hallways, shutting doors that may have been propped open, and reporting a co-worker who is acting in an odd manner. Some organizations deliberately stage suspicious situations to see which employees respond correctly to them. Those who do get some token reward; those who don't get additional training.

Trust But Verify

As with logical security, the principles of zero trust and trust but verify can (and oftentimes) coexist within the same organization when it comes to physical security. Perhaps the most common implementation of the principle of trust but verify is the logging of physical events, which are then periodically checked by someone else. For example, if there is a safe or area that needs to be locked after work hours, it could be the responsibility of one individual to lock it (maybe the last one out) and another to verify that it was locked (maybe a security guard or rotating staff member assigned to after-hours checks).

The critical aspect of this principle is to actually verify that individuals are carrying out their responsibilities. For example, is anyone checking the physical access logs periodically and comparing them to what should be happening? Are employees who are on vacation badging in? This could indicate a stolen badge. Is a staff member coming in at odd hours for no apparent reason? In multiple, documented cases this has happened because employees were doing something they didn't want others noticing. Think of your own organization. Are there any things you or your team should be verifying regularly with regard to physical security? If not, should there be?

Shared Responsibility

Of course, not every aspect of site and facility security will rest on your shoulders as a security professional. In many cases, organizations share this responsibility with partners, landlords, and service providers. If you share office space in a building, whoever owns the building has certain responsibilities for its security. They may provide lobby guards and ensure that all the perimeter doors are locked except those leading to authorized access points. Or perhaps guards are provided to your organization by a security firm. They will have clearly defined responsibilities documented in the contract or service agreement.

All too often, however, the delineation of shared responsibilities is not clearly understood by all who should. A good way to discover points of confusion is to regularly conduct physical security drills, such as physical penetration tests and tabletop exercises involving all responsible entities, perhaps extending to local law enforcement as appropriate.

Separation of Duties

Duties can be deliberately separated with regard to physical security to mitigate theft and unauthorized physical access, among other risks. As an example, it is common for organizations to require one person (typically a receptionist or guard) to sign in guests and another person to escort them. This reduces the risk that a malicious insider sneaks in an external conspirator unnoticed. It also means that there are two pairs of eyes on each visitor to minimize the chances of accidentally letting an impostor in. Another example of separation of duties concerns receiving shipments. If only one person is involved in the process, how would we know whether a shipment that person reports as incomplete was truly incomplete or that person is stealing? To prevent this from easily happening, some organizations require only one person to sign for the delivery but require at least one other person to be present when the packages are opened and the property is added to the inventory.

Least Privilege

We previously mentioned the need to balance security with functionality, and this is especially true when it comes to staff authorizations. Staff should have the least amount of privileges that are absolutely necessary for their jobs, while enabling them to do those jobs efficiently and effectively. When it comes to site and facility security, this commonly takes the form of access to restricted areas. If employees have to badge in and out of different facilities, it is important to ensure that each staff member can effortlessly flow through the ones in which they do their jobs, and no others. For example, if some employees work at site A, their badges should not allow them entry to site B unless it is required.

Another example that comes to mind is access to server rooms or data centers. Oftentimes the racks that house the computing and storage devices in these facilities can and should be locked. Depending on the devices involved and their purpose, it is typical for different groups to need access to different racks. For example, the IT team may need access to the racks containing the domain controller and mail servers. The product team may need to get to the development servers that are on a different rack and subnet. The security team may need access to the security appliances, such as the network detection and response systems. Obviously, these groups probably shouldn't be able to access all the devices in the facility, but only the ones they need to do their jobs. Rather than leave all racks unlocked or use the same key for expediency, these staff members should be given only the minimum access possible to just the resources they need.

Simplicity

We discussed in Chapter 9 how complexity leads to the introduction of defects that, in turn, could create vulnerabilities. When it comes to our sites and facilities, the need for simplicity comes in at least two flavors: layout and procedural. The simpler the layout of our workplaces, the fewer hiding spots we create, the fewer cameras we need, and the more eyes that will naturally fall on everything that happens there. Whenever you have the choice, choose the simpler, more open layout to improve your organization's physical security.

Regardless of whether or not you can control the layout of your sites and facilities, you can almost always influence the security procedures that are implemented. Of course, you want to make these procedures so simple that they become second nature to all your organization's staff. From signing in and escorting visitors to safely evacuating the building in case of emergency, your organization needs procedures that are as simple as possible. These are normally validated and practiced during drills, which also provide a good opportunity to verify that no unnecessary complexity has crept into them.

Secure Defaults

As discussed in Chapter 9, secure defaults mean everything starts off in a place of extreme security that is then intentionally loosened until people can get their jobs done, but no further. Picture, then, your site schematics. Fence in every outdoor area, block off all vehicular travel around it, lock every door, and keep everyone out of every space. In other words, lock the place down as tightly as you know how. Now, take one of your teams, say IT, and walk through a day in their life. As you step through it, make note of how they'd drive in, what doors they'd have to use, which locks they need to open, and where they need to sit. Repeat this process for each organizational team, and then for your partners, vendors, and general visitors. You'll end up with the minimal relaxation to your extreme security plan that would be required for your staff members to do their jobs. This is what secure defaults look like for site security planning.

Fail Securely

This is a good point to discuss the difference between two principles that sound a lot alike but have very different implications. Recall that a *fail-secure* configuration is one in which things like doors default to being locked if there are any problems with the power, because that is the highest level of security for that system (the lock). If people do not need to use specific doors for escape during an emergency, then those doors can most likely default to fail-secure settings. On the other hand, a *fail-safe* setting means that if a power disruption occurs that affects the automated locking system, the doors default to being unlocked. Fail-safe deals directly with protecting people. If people work in an area in which a fire starts or the power is lost, it is a terrible idea to lock them in. Doorways with automatic locks can be configured in either mode, but we need to make careful decisions about which is appropriate and how we mitigate residual risks when we execute a fail-safe setting.

EXAM TIP The protection of human life trumps everything else. Be on the lookout for exam questions involving fail-safe versus fail-secure configurations.

Privacy by Design

Finally, we must keep in mind the need for privacy as we plan our site and facility security. This comes up in a number of areas and, frankly, varies widely between organizations. On one end of the spectrum, we have military and intelligence agencies wherein privacy in physical spaces is very limited due to the nature of the work being done. On the other end, consider healthcare organizations, in which privacy is absolutely essential. Regardless of where your organization falls in that spectrum, privacy definitely plays some role (e.g., restrooms) in shaping the manner in which you develop your site security. At a minimum, you should consider what private conversations (e.g., employee counseling, patient intakes, etc.) will take place in your site and where those would take place.

The Site Planning Process

Site and facility planning involves much more than physical security. Organizations should also be addressing issues like functionality, efficiency, cost, compliance, and aesthetics, just to name a few. However, as these (and other) issues are being addressed by the planning team, it is best to consider how each relates to physical security. For example, functionality and efficiency can frequently hinder security (and vice versa). So, we should balance the various requirements to ensure we are enabling the organization's functions while also protecting it from the various threats we've modeled for it. These threats include the following:

- **Natural environmental threats** Floods, earthquakes, storms, volcanic eruptions, pandemics, and so forth
- **Supply system threats** Power distribution outages, communications interruptions, and interruption of other resources such as water, gas, and air filtration
- **Manmade threats** Deliberate or accidental actions of humans, including fire, burglary, equipment loss/destruction, active shooters, and even terrorism

In all situations, the primary consideration, above all else, is that nothing should impede *life safety* goals. Protecting human life is the first priority. Good planning helps balance life safety concerns and other security measures. For example, barring a door to prevent unauthorized physical intrusion might prevent individuals from being able to escape in the event of a fire. Life safety goals should always take precedence over all other types of goals; thus, this door might allow insiders to exit through it after pushing an emergency bar, but not allow external entities in.

As with any type of security, most attention and awareness surround the exciting and headline-grabbing tidbits about large crimes being carried out and criminals being captured. In information security, most people are aware of viruses and hackers, but not of the components that make up a corporate security program. The same is true for physical security. Many "water cooler" conversations include talk about current robberies, murders, and other criminal activity, but not much attention is paid to the necessary framework that should be erected and maintained to reduce these types of activities.

An organization's physical security program should address the following goals:

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

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

This all sounds straightforward enough, until the team responsible for developing the physical security program looks at all the possible threats, the finite budget that the team has to work with, and the complexity of choosing the right combination of countermeasures and ensuring that they all work together in a manner that ensures no gaps of protection. All of these components must be understood in depth before the design of a physical security program can begin.

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

- Number of crimes committed
- Number of disruptions experienced
- Number of crimes attempted
- Number of disruptions prevented
- Time between detection, assessment, and recovery steps

- Business impact of disruptions
- Number of false-positive detection alerts
- Time it took for a criminal to defeat a control
- Time it took to restore the operational environment
- Financial loss of a successful crime
- Financial loss of a successful disruption

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

NOTE Metrics are important in all domains of security because organizations need to allocate the necessary controls and countermeasures to mitigate risks in a cost-beneficial manner. You can't manage what you can't measure.

The physical security team needs to carry out a risk analysis, which will identify the organization's vulnerabilities, threats, and business impacts. The team should present these findings to management and work with management to define an acceptable risk level for the physical security program. From there, the team must develop baselines (minimum levels of security) and metrics in order to evaluate and determine if the baselines are being met by the implemented countermeasures. Once the team identifies and implements the countermeasures, the performance of these countermeasures should be continually evaluated and expressed in the previously created metrics. These performance values are compared to the set baselines. If the baselines are continually maintained, then the security program is successful because the organization's acceptable risk level is not being exceeded. This is illustrated in Figure 10-1.

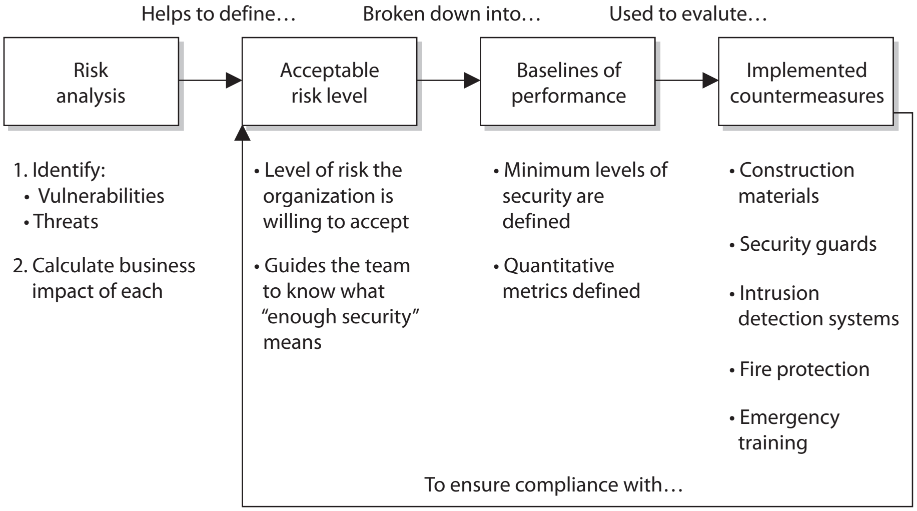

Helps to define…
Broken down into…
Used to evalute…
Risk analysis
Acceptable risk level
Baselines of performance
Implemented countermeasures
1. Identify:
• Vulnerabilities
• Threats
2. Calculate business impact of each
• Level of risk the organization is willing to accept
• Guides the team to know what "enough security" means
• Minimum levels of security are defined
• Quantitative metrics defined
• Construction materials
• Security guards
• Intrusion detection systems
• Fire protection
• Emergency training
To ensure compliance with…

Figure 10-1 Relationships of risk, baselines, and countermeasures

Similarities in Approaches

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

Each requires a solid risk analysis process. Review Chapter 2 to understand the core components of every risk analysis.

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

1. Identify a team of internal employees and/or external consultants who will build the physical security program through the following steps.
2. Define the scope of the effort: site or facility.
3. Carry out a risk analysis to identify the vulnerabilities and threats and to calculate the business impact of each threat.
4. Identify regulatory and legal requirements that the organization must meet and maintain.
5. Work with management to define an acceptable risk level for the physical security program.
6. Derive the required performance baselines from the acceptable risk level.
7. Create countermeasure performance metrics.
8. Develop criteria from the results of the analysis, outlining the level of protection and performance required for the following categories of the security program:
   - Deterrence
   - Delaying
   - Detection
   - Assessment
   - Response
9. Identify and implement countermeasures for each program category.
10. Continuously evaluate countermeasures against the set baselines to ensure the acceptable risk level is not exceeded.

Legal Requirements

In physical security there are some regulatory and high-level legal requirements that must be met, but many of them just have high-level statements, as in "protect personnel" or "implement lifesaving controls." It is up to the organization to figure out how to actually meet these requirements in a practical manner. In the United States there is a lot of case law that pertains to physical security requirements, which is built upon precedence. This means that there have been lawsuits pertaining to specific physical security instances and a judgment was made on liability. For example, there is no law that dictates that you must put up a yellow sign indicating that a floor is wet. Many years ago someone somewhere slipped on a wet floor and sued the company, and the judge ruled that the company was negligent and liable for the person's injuries because it didn't warn the person about the wet floor. Now it is built into many company procedures that after a floor is mopped or there is a spill, this yellow sign is put in place so no one will fall and sue the company. It is hard to think about and cover all of these issues since there is no specific checklist to follow. This is why it is a good idea to consult with a physical security expert when developing a physical security program.

Once these steps have taken place, the team is ready to move forward in its actual design phase. The design will incorporate the controls required for each category of the program: deterrence, delaying, detection, assessment, and response. We will dig deeper into these categories and their corresponding controls later in the chapter in the section "Designing a Physical Security Program."

One of the most commonly used approaches in physical security program development is described in the following section.

Crime Prevention Through Environmental Design

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

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

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

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

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

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

If a parking garage were developed using the CPTED approach, the stair towers and elevators within the garage might have glass windows instead of metal walls, so people would feel safer, and potential criminals would not carry out crimes in this more visible environment. Pedestrian walkways would be created such that people could look out across the rows of cars and see any suspicious activities. The different rows for cars to park in would be separated by low walls and structural pillars, instead of solid walls, to allow pedestrians to view activities within the garage. The goal is to not provide any hidden areas where criminals can carry out their crimes and to provide an open-viewed area so if a criminal does attempt something malicious, there is a higher likelihood of someone seeing it.

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

Natural Access Control

Natural access control is the guidance of people entering and leaving a space by the placement of doors, fences, lighting, and even landscaping. For example, an office building may have external bollards with lights in them, as shown in Figure 10-2. These bollards actually carry out different safety and security services. The bollards themselves protect

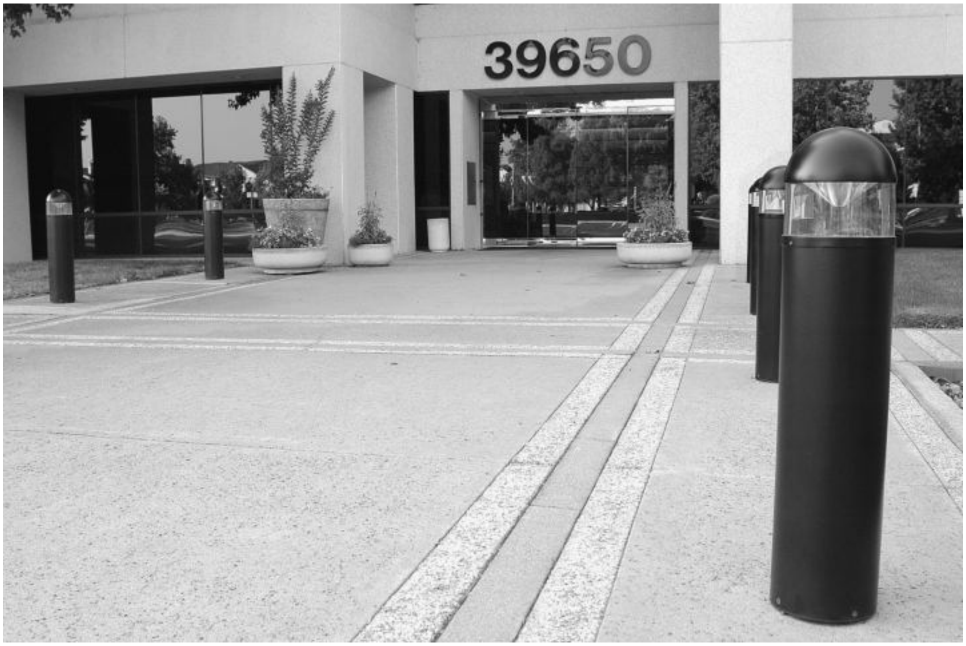


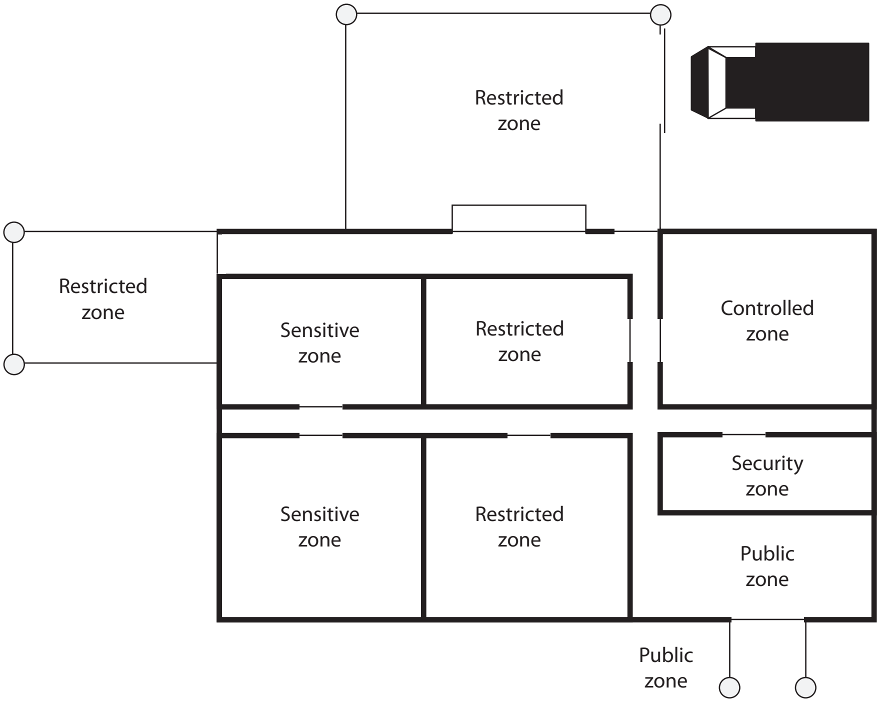
Figure 10-2 Sidewalks, lights, and landscaping can be used for protection.

the facility from physical destruction by preventing people from driving their cars into the building. The light emitted helps ensure that criminals do not have a dark place to hide. And the lights and bollard placement guide people along the sidewalk to the entrance, instead of using signs or railings. As shown in Figure 10-2, the landscape, sidewalks, lighted bollards, and clear sight lines are used as natural access controls. They work together to give individuals a feeling of being in a safe environment and help dissuade criminals by working as deterrents.

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

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

The CPTED model shows how *security zones* can be created. An environment's space should be divided into zones with different security levels, depending upon who needs to be in that zone and the associated risk. The zones can be labeled as controlled, restricted, public, or sensitive. This is conceptually similar to asset classification, as described in Chapter 5, in which different classifications are created, along with data handling procedures and the level of protection that each classification requires. The same is true of physical zones. Each zone should have a specific protection level required of it, which will help dictate the types of controls that should be put into place.



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

- Limit the number of entry points.
- Force all guests to go to a front desk and sign in before entering the environment.
- Reduce the number of entry points even further after hours or during the weekend, when not as many employees are around.
- Implement sidewalks and landscaping to guide the public to a main entrance.
- Implement a back driveway for suppliers and deliveries that is not easily accessible to the public.
- Provide lighting for the pathways the public should follow to enter a building to help encourage use of only one entry for access.

- Implement sidewalks and grassy areas to guide vehicle traffic to only enter and exit through specific locations.
- Provide parking in the front of the building (not the back or sides) so people will be directed to enter the intended entrance.

These types of access controls are used all of the time, and we usually do not think about them. They are built into the natural environment to manipulate us into doing what the owner of the facility wants us to do. When you are walking on a sidewalk that leads to an office front door and there are pretty flowers on both sides of the sidewalk, know that they are put there because people tend not to step off a sidewalk and crush pretty flowers. Flowers are commonly placed on both sides of a sidewalk to help ensure that people stay on the sidewalk. Subtle and sneaky, but these control mechanisms work.

More obvious access barriers can be naturally created (cliffs, rivers, hills), existing manmade elements (railroad tracks, highways), or artificial forms designed specifically to impede movement (fences, closing streets). These can be used in tandem or separately to provide the necessary level of access control.

Natural Surveillance

Surveillance can also take place through organized means (security guards), mechanical means (security cameras), and natural strategies (straight lines of sight, low landscaping, raised entrances). The goal of *natural surveillance* is to make criminals feel uncomfortable by providing many ways observers could potentially see them and to make all other people feel safe and comfortable by providing an open and well-designed environment.

Natural surveillance is the use and placement of physical environmental features, personnel walkways, and activity areas in ways that maximize visibility. Figure 10-3 illustrates a stairway in a parking garage designed to be open and allow easy observation.

Next time you are walking down a street and see a bench next to a building or you see a bench in a park, know that the city has not allocated funds for these benches just in case your legs get tired. These benches are strategically placed so that people will sit and watch other people. This is a very good surveillance system. The people who are watching others do not realize that they are actually protecting the area, but many criminals will identify them and not feel as confident in carrying out some type of malicious deed.

Walkways and bicycle paths are commonly installed so that there will be a steady flow of pedestrians who could identify malicious activity. Buildings might have large windows that overlook sidewalks and parking lots for the same reason. Shorter fences might be installed so people can see what is taking place on both sides of the fence. Certain high-risk areas have more lighting than what is necessary so that people from a distance can see what is going on. These high-risk areas could be stairs, parking areas, bus stops, laundry rooms, children's play areas, dumpsters, and recycling stations. These constructs help people protect people without even knowing it.

Territorial Reinforcement

The third CPTED strategy is *territorial reinforcement*, which creates physical designs that emphasize or extend the organization's physical sphere of influence so legitimate users feel a sense of ownership of that space. Territorial reinforcement can be

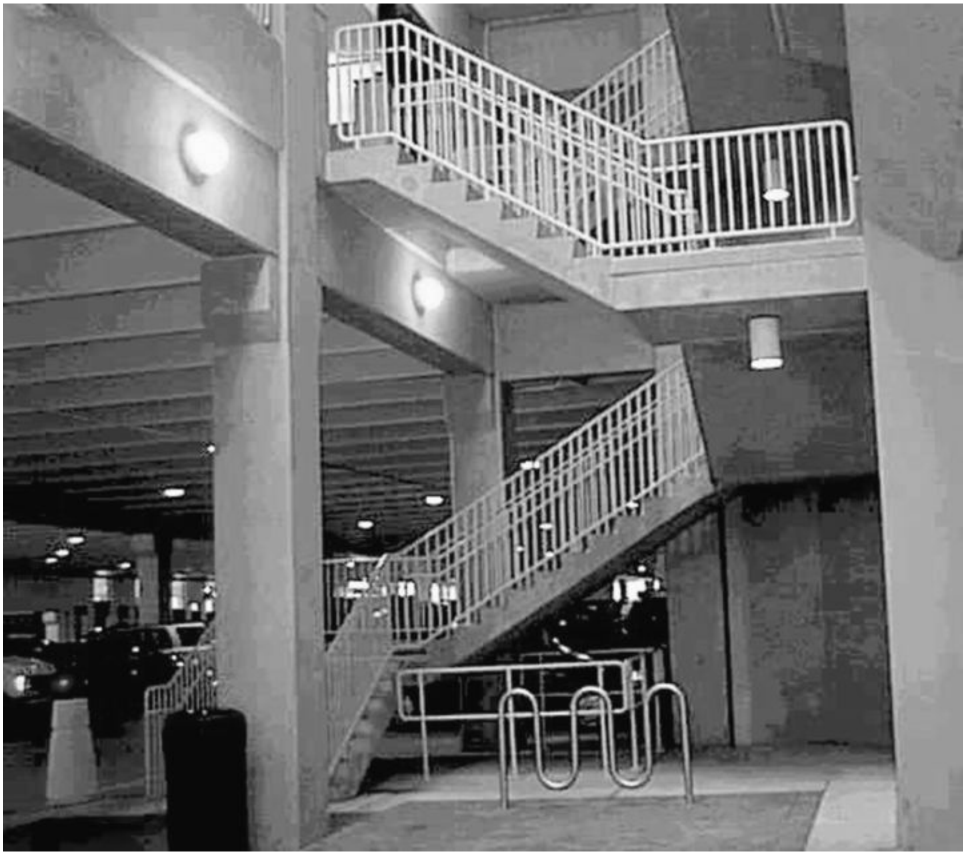


Figure 10-3 Open areas reduce the likelihood of criminal activity.

implemented through the use of walls, fences, landscaping, light fixtures, flags, clearly marked addresses, and decorative sidewalks. The goal of territorial reinforcement is to create a sense of a dedicated community. Organizations implement these elements so employees feel proud of their environment and have a sense of belonging, which they will defend if required to do so. These elements are also implemented to give potential offenders the impression that they do not belong there, that their activities are at risk of being observed, and that their illegal activities will not be tolerated or ignored.

Most corporate environments use a mix of the CPTED and target-hardening approaches. CPTED deals mainly with the construction of the facility, its internal and external designs, and exterior components such as landscaping and lighting. If the environment is built based on CPTED, then the target hardening is like icing on the cake. The target-hardening approach applies more granular protection mechanisms, such as locks and motion detectors.

Maintenance

In the mid-1980s, crime was rampant in New York City subways. Looking for creative solutions, the Metropolitan Transit Authority (MTA) hired George L. Kelling as a consultant. Kelling had written an influential book titled *Broken Windows* in which he presented his theory that visible signs of crime create an environment that encourages more crime. Make the signs go away, the theory goes, and so does the crime. In a large-scale experiment involving the "broken windows" theory that extended into 2001, NYC saw a dramatic decrease in crime, which strongly suggested the theory is valid.

The fourth and final CPTED strategy, *maintenance*, is an extension of the broken windows theory. It basically states that criminals will be more attracted to facilities that look unkept because they'll assume that the occupants don't care as much about them and probably lack the resources to properly maintain and secure them. Faced with a well-kept facility with no burned-out lamps, no broken windows, and with manicured lawns, criminals will think those inside the facility are more attentive, well resourced, and possibly alert.

Designing a Physical Security Program

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

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

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

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

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

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

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

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

By this point, the team has carried out a risk analysis, which consisted of identifying the organization's vulnerabilities, threats, and business impact pertaining to the identified threats. The program design phase should begin with a structured outline, which will evolve into a framework. This framework will then be fleshed out with the necessary controls and countermeasures. The outline should contain the program categories and the necessary countermeasures. The following is a simplistic example:

I. Deterrence of criminal activity

- **A.** Fences
- **B.** Warning signs
- **C.** Security guards
- **D.** Dogs

II. Delay of intruders to help ensure they can be caught

A. Locks

B. Defense-in-depth measures

C. Access controls

III. Detection of intruders

A. External intruder sensors

B. Internal intruder sensors

IV. Assessment of situations

A. Security guard procedures

B. Damage assessment criteria

V. Response to intrusions and disruptions

A. Communication structure (calling tree)

B. Response force

C. Emergency response procedures

D. Police, fire, medical personnel

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

Facility

When an organization decides to erect a building, it should consider several factors before pouring the first batch of concrete. Of course, it should review land prices, customer population, and marketing strategies, but as security professionals, we are more interested in the confidence and protection that a specific location can provide. Some organizations that deal with top-secret or confidential information and processes make their facilities unnoticeable so they do not attract the attention of would-be attackers. The building may be hard to see from the surrounding roads, the organization's signs and logos may be small and not easily noticed, and the markings on the building may not give away any information that pertains to what is going on inside that building. It is a type of urban camouflage that makes it harder for the enemy to seek out that organization as a target. This is very common for telecommunication facilities that contain critical infrastructure switches and other supporting technologies. When driving down the road you might pass three of these buildings, but because they have no features that actually stand out, you likely would not even give them a second thought—which is the goal.

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

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

In the United States there is an Air Force base built into a mountain close to Colorado Springs, Colorado. The underground Cheyenne Mountain complex is made up of buildings, rooms, and tunnels. It has its own air intake supply, as well as water, fuel, and sewer lines. This is where the North American Aerospace Defense Command (NORAD) carries out its mission and apparently, according to many popular movies, is where you should be headed if the world is about to be blown up.

Construction

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

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

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

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

Walls:

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

Doors:

- Combustibility of material (wood, pressed board, aluminum)
- Fire rating
- Resistance to forcible entry
- Emergency marking
- Placement
- Locked or controlled entrances
- Alarms
- Secure hinges
- Directional opening
- Electric door locks that revert to an unlocked state for safe evacuation in power outages
- Type of glass—shatterproof or bulletproof glass requirements

Ceilings:

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

Windows:

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

Flooring:

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

Heating, ventilation, and air conditioning:

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

Electric power supplies:

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

Water and gas lines:

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

Fire detection and suppression:

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

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

Heavy timber construction material is sometimes used for office buildings. Combustible lumber is still used in this type of construction, but there are requirements on the thickness and composition of the materials to provide more protection from fire. The construction materials must be at least 4 inches in thickness. Denser woods are used and are fastened with metal bolts and plates. Whereas light frame construction material has a fire survival rate of 30 minutes, the heavy timber construction material has a fire survival rate of one hour.

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

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

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

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

Entry Points

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

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

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

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

Doors Different door types for various functionalities include the following:

- Vault doors
- Personnel doors
- Industrial doors
- Vehicle access doors
- Bullet-resistant doors

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

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

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

Fire codes dictate the number and placement of doors with panic bars on them. These are the crossbars that release an internal lock to allow a locked door to open. Panic bars can be on regular entry doors and also on emergency exit doors. Those are the ones that usually have the sign that indicates the door is not an exit point and that an alarm will go off if the door is opened. It might seem like fun and a bit tempting to see if the alarm will *really* go off or not—but don't try it. Security people are not known for their sense of humor.

Mantraps and turnstiles can be used so unauthorized individuals entering a facility cannot get in or out if it is activated. A *mantrap* is a small room with two doors. The first door is locked; a person is identified and authenticated by a security guard, biometric system, smart card reader, or swipe card reader. Once the person is authenticated and access is authorized, the first door opens and allows the person into the mantrap. The first door locks and the person is trapped. The person must be authenticated again before the second door unlocks and allows him into the facility. Some mantraps use biometric systems that weigh the person who enters to ensure that only one person at a time is entering the mantrap area. This is a control to counter piggybacking.

Window Types Though most of us would probably think of doors as the obvious entry points, windows deserve every bit as much attention in the design of secure facilities. Like doors, different types of windows afford various degrees of protection against intrusions. The following sums up the types of windows that can be used:

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

Site and Facility Controls

Having covered the general processes and principles we should use in planning security for our sites and facilities, we now turn our attention to examples of specific controls we should consider. The following section discuss the most common or important controls you should know both for the exam and in the conduct of your job.

Work Area Security

The largest total area in an organization's facilities is usually devoted to workspaces for its staff. In terms of facility security, these spaces comprise the largest attack surface for the organization. This is where malicious insiders, thieves, and active shooters will find the most target-rich environment. For this reason, we need to consider the threats to our workforce occupying those spaces and implement controls to keep them and their assets protected. Just like we segment our networks to limit where digital intruders can operate, we should separate our workspaces to make it harder for physical intruders to accomplish their objectives. *Internal partitions* are used to create barriers between one area and another. These partitions can be used to segment separate work areas, but should not be used in protected areas that house sensitive systems and devices because they would limit the ability to detect malicious activity on those systems.

Movement from one area to another should ideally be restricted using *keycard entry systems*, which are electronic locks that are unlocked by keycards. Keycards are plastic cards with magnetic or radio frequency identification (RFID) components that act as physical keys on special electronic locks. Alternatively, doors between areas could be remotely locked and unlocked by security guards to restrict the movement of an assailant, protect occupants, or facilitate evacuations. To facilitate this remote operation, all work areas should be covered by security cameras that automatically record all activity and save the video files, at least for several days.

Beware of the dropped ceilings that many office buildings have. These can cause the interior partitions or even walls to not extend to the true ceiling—only to the dropped ceiling. An intruder can lift a ceiling panel and climb over the partition. This example of intrusion is shown in Figure 10-4. In many situations, this would not require forced entry, specialized tools, or much effort. (In some office buildings, this may even be possible from a common public-access hallway.) These types of internal partitions should not be relied upon to provide protection for sensitive areas.

Another common control for work areas is a clean desk policy. This means that, before staff members leave their desks for extended periods (e.g., lunch, end of day), they remove all documents and pilferable items and store them in locked drawers. This ensures that sensitive documents are not lying around for wandering eyes (or cameras) to see. At the

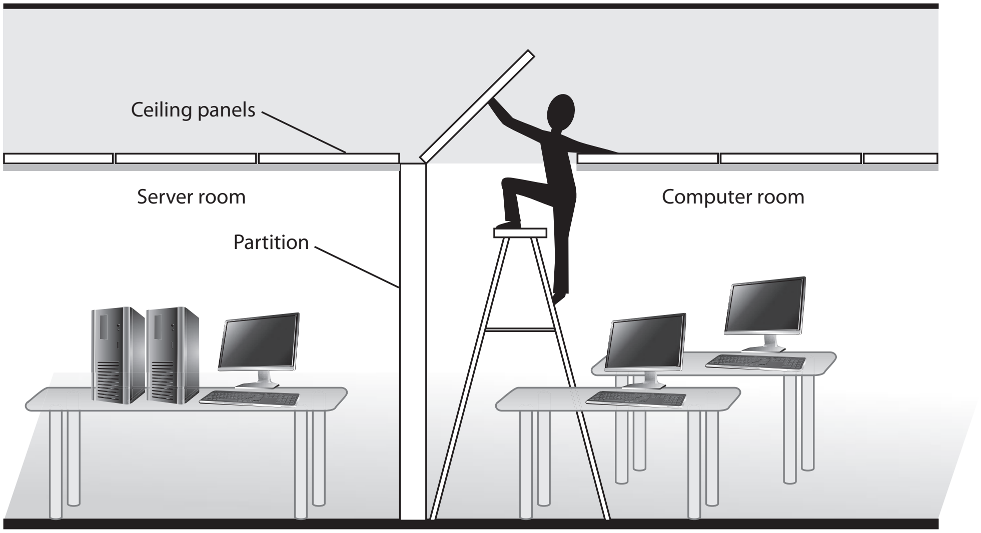


Figure 10-4 An intruder can lift ceiling panels and enter a secured area with little effort.

Restricted Areas

In some cases, a work area can be so sensitive that we must take extreme measures to ensure only authorized personnel are allowed in. Examples of these types of work areas are sensitive compartmented information facilities (SCIFs) used by governments to protect top secret information; police crime labs, where the integrity of evidence is absolutely paramount; research and development laboratories conducting particularly sensitive work; and many data centers. The controls we would use in these sensitive areas are similar to the ones previously discussed but are much stricter and more rigorously enforced.

end of the shift or work day, somebody is assigned the task of checking all desks to ensure compliance with the policy.

Data Processing Facilities

With the growing trend toward cloud computing, data processing facilities such as server rooms and data centers are less common than once was the case. Still, many organizations, not to mention providers of cloud services, can't get away from having these facilities. Since most servers, routers, switches, mainframes, and data centers can be controlled remotely and seldom require physical interaction, our data processing facilities have few people milling around and potentially spilling coffee. This lack of personnel sitting and working in them for long periods means these data centers can be constructed in a manner that is efficient for equipment instead of people.

On the other hand, there are situations in which people may have to be physically in the data center, perhaps for very extended periods of time (equipment installations/upgrades, data center infrastructure upgrades and reconfigurations, incident response, forensic data acquisition, etc.). Consequently, the inhospitable conditions (cold, dry environment; lack of comfortable workspaces; extremely high decibel levels) should be taken into account when deploying such personnel.

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

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

Because data centers usually hold expensive equipment and the organization's critical data, their protection should be thoroughly thought out before implementation. A data center should not be located on an upper floor of a building, because that would make accessing it in a timely fashion in case of a fire more difficult for an emergency crew. By the same token, data centers should not be located in basements where flooding can affect the systems. And if a facility is in a hilly area, the data center should be located well above ground level. Data centers should be located at the core of a building so that if there is some type of attack on the building, the exterior walls and structures will absorb the hit and hopefully the data center will not be damaged.

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

The various controls discussed next are shown in Figure 10-5. The team responsible for designing a new data center (or evaluating a current data center) should understand all the controls shown in Figure 10-5 and be able to choose what is needed.

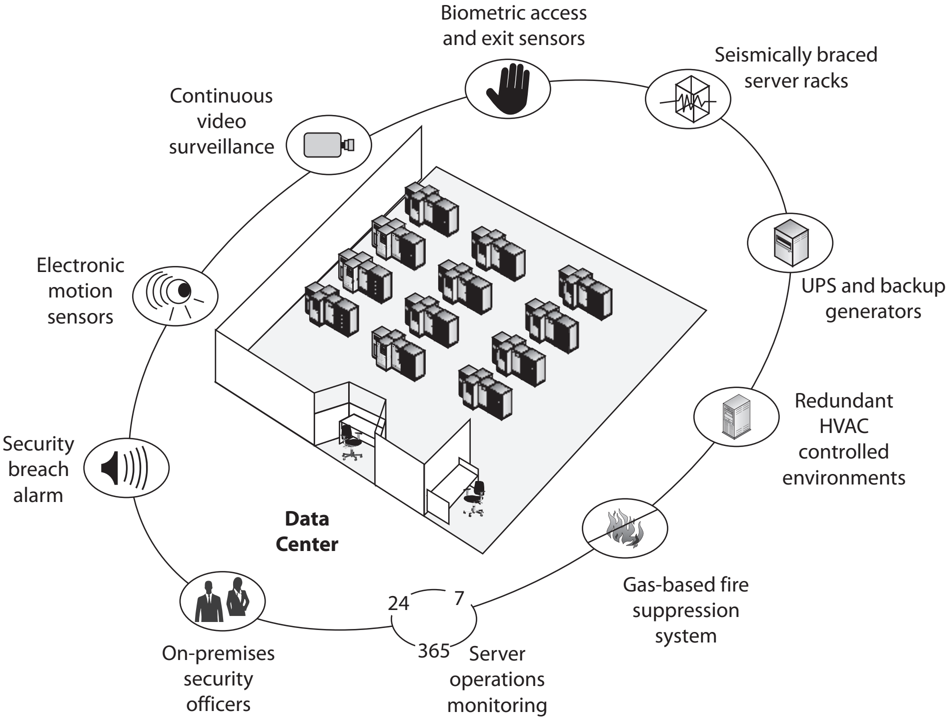

Biometric access and exit sensors
Seismically braced server racks
Continuous video surveillance
UPS and backup generators
Electronic motion sensors
Redundant HVAC controlled environments
Security breach alarm
Data Center
Gas-based fire suppression system
24
7
365
On-premises security officers
Server operations monitoring

Figure 10-5 A data center should have many physical security controls.

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

Smoke detectors or fire sensors should be implemented, and portable fire extinguishers should be located close to the equipment and should be easy to see and access (see "Fire Safety" later in the chapter for details). Water sensors should be placed under the raised floors. Since most of the wiring and cables run under the raised floors, it is important that water does not get to these places and, if it does, that an alarm sound if water is detected.

TIP If there is any type of water damage in a data center or facility, mold and mildew could easily become a problem. Instead of allowing things to "dry out on their own," many times it is better to use industry-strength dehumidifiers, water movers, and sanitizers to ensure secondary damage does not occur.

Water can cause extensive damage to equipment, flooring, walls, computers, and facility foundations. It is important that an organization be able to detect leaks and unwanted water. The detectors should be under raised floors and on dropped ceilings (to detect leaks from the floor above it). The location of the detectors should be documented, and their position marked for easy access. As smoke and fire detectors should be tied to an alarm system, so should water detectors. The alarms usually just alert the necessary staff members and not everyone in the building. The staff members who are responsible for following up when an alarm sounds should be trained properly on how to reduce any potential water damage. Before anyone pokes around to see where water is or is not pooling in places it does not belong, the electricity for that particular zone of the building should be temporarily turned off.

Water detectors can help prevent damage to

- Equipment
- Flooring
- Walls
- Computers
- Facility foundations

Location of water detectors should be

- Under raised floors
- On dropped ceilings

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

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

Data centers need to have their own backup power supplies, either an uninterrupted power supply (UPS) or generators. The different types of backup power supplies are discussed later in the chapter, but it is important to know at this point that the power backup must be able to support the load of the data center.

Many organizations choose to use large glass panes for the walls of the data center so personnel within the center can be viewed at all times. This glass should be shatter-resistant since the window is acting as an exterior wall. The center's doors should not be hollow, but rather secure solid-core doors. Doors should open out rather than in, so they don't damage equipment when opened. Best practices indicate that the door frame should be fixed to adjoining wall studs and that there should be at least three hinges per door. These characteristics would make the doors much more difficult to break down.

Distribution Facilities

Distribution facilities are systems that distribute communications lines, typically dividing higher-bandwidth lines into multiple lower-bandwidth lines. A building typically has one main distribution facility (MDF) where one or more external data lines are fed into the server room, data center, and/or other smaller intermediate distribution facilities (IDFs). An IDF usually provides individual lines or drops to multiple endpoints, though it is possible to daisy-chain IDFs as needed.

Larger IDFs are usually installed in small rooms normally called *wiring closets*. All of the design considerations for unstaffed server rooms and data centers discussed in the previous section also apply to these facilities. It is critical to think of these as the sensitive IT facilities that they are and not as just closets. We've seen too many organizations that allow their IDF rooms to do double duty as janitors' closets.

Smaller IDFs are oftentimes installed in rooms that have a large number of network endpoints. They can be as small as a single switch and small patch panel on a shelf or as big as a cabinet. Unlike an MDF, an IDF is usually not enclosed in its own room, which makes it more susceptible to tampering and accidental damage. Whenever possible, an IDF should be protected by a locked enclosure. Ideally, it is elevated to reduce the risk of flood or collision damage and to make it more visible should someone tamper with it. Another consideration that is oftentimes overlooked is placing the IDF away from overhead sprinklers, pipes, or HVAC ducts.

Storage Facilities

Storage facilities are often overlooked when it comes to security considerations other than, perhaps, locking them. While a simple lock may be all we need to think of when we're storing office supplies and basic tools, we should really think about what it is that we are protecting. In many cases, the physical locks we use are either low grade (in other words, easily picked) or have keys that are shared by multiple people. Unlike their modern electronic counterparts, these locks lack built-in auditing tools to see who opened them and when. If you are storing anything that you'd hate to have go missing, you probably want to think long and hard about who gets a key, how it's signed out, and how to periodically inventory the storage area.

This is particularly true of storage facilities in which you store computing equipment. Depending on your organizational procedures, you may be storing computers with storage devices that have not yet been securely wiped or baselined. This means there are security risks if someone gets their hands on them apart from that of theft. You also need to worry about the environmental conditions of the storage facility, since computers don't do so well in hot, humid areas over long periods.

These are just examples to get you thinking. Whatever is stored in the facility should impact the security controls you put on it. There are two types of storage facilities that deserve special attention, which are those we use to store media and those we use to store evidence. Let's take a closer look at each.

Media Storage

We discussed in Chapter 5 that the information life cycle includes an archival phase during which information is not regularly used but we still need to retain it. This happens, for example, when we close accounts but still need to keep the records for a set number of years, or when we do backups. In any event, we have to keep a large number of disks, magnetic tapes, or even paper files for prolonged periods until we either need them or are able to dispose of them. This has to happen in a secure location that meets the requirements discussed for server rooms and data centers. Unfortunately, media storage is sometimes not given the importance it deserves, which can result in the loss or compromise of important information.

Evidence Storage

Evidence storage facilities are even more sensitive because any compromise, real or perceived, could render evidence inadmissible in court. We will cover forensic investigations in Chapter 22, but every organization with a dedicated IT staff should probably have a secure facility in which to store evidence. The two key requirements for evidence storage facilities are that they are properly secured and that all access and transfers are logged.

Ideally, only select incident handlers and forensic investigators have access to the facility. Unless forensic investigations are part of your business, you will likely only need a rugged cabinet with a good lock and a register in which to record who opened/closed it and what was done in it. This is yet another example of a situation in which a technical control alone (like the cabinet or safe) won't do the job. You also have to have a good policy (like logging all access to the contents) that is rigorously enforced.

Utilities

Utilities, as with storage, is another area on which many of us don't spend a lot of time thinking about security. Still, utilities can pose significant risks to our sites and facilities. Local construction codes may address safety issues, but they do very little to otherwise help us protect our organizations.

Water and Wastewater

As the saying goes, water is life. Without clean water and wastewater services, our staffed facilities would not be able to operate safely for any length of time. Interruptions to these services, therefore, could require the evacuation of most or all personnel from a facility, which could degrade its security posture and create a window of opportunity for nefarious activity.

An abundance of water in the wrong place can also cause serious problems. As we discussed previously with regard to data centers and distribution facilities, it is critical to route water pipes (or, more realistically, position assets) so that a ruptured or leaking pipe will not cause equipment damage.

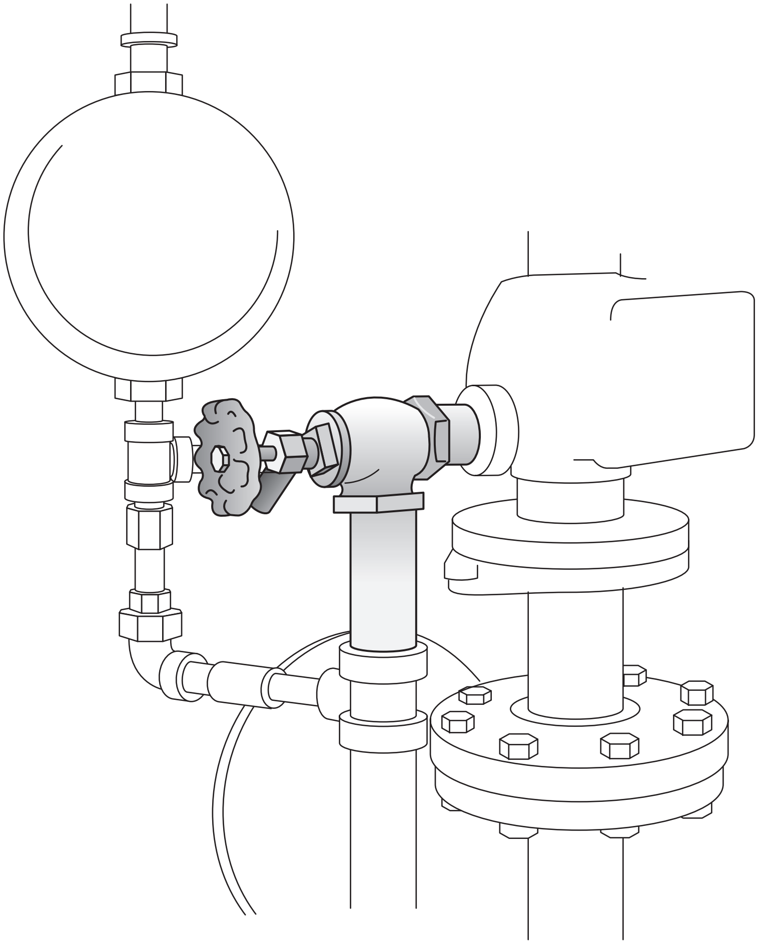
During facility construction, the physical security team must make certain that water, steam, and gas lines have proper shutoff valves, as shown in Figure 10-6, and *positive drains*, which means their contents flow out instead of in. If there is ever a break in a main water pipe, the valve to shut off water flow must be readily accessible. Similarly, in case of fire in a building, the valve to shut off the gas lines must be readily accessible. In case of a flood, an organization wants to ensure that material cannot travel up through the water pipes and into its water supply or facility. Facility, operations, and security personnel should know where these shutoff valves are, and there should be strict procedures to follow in these types of emergencies. This will help reduce the potential damage.

Electric Power

Power failure, particularly over a long stretch of time, can be devastating to an unprepared organization. Having good plans to fall back on is crucial to ensure that a business will not be drastically affected by storms, high winds, hardware failure, lightning, or other events that can stop or disrupt power supplies. A continuous supply of electricity assures the availability of organizational resources; thus, a security professional must be familiar with the threats to electric power and the corresponding countermeasures.

Power Backup Several types of power backup capabilities exist. Before you choose one, you should calculate the total cost of anticipated downtime and its effects. This information can be gathered from past records and other businesses in the same area on the same power grid and plugged into the annualized loss expectancy (ALE) formula we

Figure 10-6 Water, steam, and gas lines should have emergency shutoff valves.



discussed in Chapter 2. Essentially, you want to calculate the annual expected cost of power outages in terms of lost revenue, recovery costs, and the like. This amount will tell you whether it makes sense to run a secondary line that is fed by a different grid or to buy a backup generator, both of which are significant investments.

If you plan to buy a generator, you also have to determine how long it will be expected to run each year, which tells you how big of a fuel storage tank you need and what the expected fuel costs are. Keep in mind that you will have to periodically run the generator to ensure that it remains ready, and also be aware that some fuels go bad after sitting around for several months. As always, we have to ensure the cure is not worse than the illness.

Just having a generator in the backyard should not give you that warm fuzzy feeling of protection. An alternative power source should be tested periodically to make sure it works and to the extent expected. Power interruption drills should be performed periodically to avoid nasty surprises. It is never good to find yourself in an emergency only to discover that the organization added a bunch of power-hungry assets since you bought the generator and it is now too small to power them all.

Electric Power Issues Electric power enables us to be productive and functional in many different ways, but if it is not installed, monitored, and respected properly, it can do us great harm. When *clean* power is being provided, the power supply contains no interference or voltage fluctuation. The possible types of interference (*line noise*) are *electromagnetic interference (EMI)* and *radio frequency interference (RFI)*, which can cause disturbance to the flow of electric power while it travels across a power line, as shown in Figure 10-7.

EMI is the effect of unwanted energy on an electrical system caused by radiations from another, nearby, electrical system. EMI can be created by the difference between three wires—hot, neutral, and ground—and the magnetic field they create. Lightning and electrical motors can induce EMI, which could then interrupt the proper flow of electrical current as it travels over wires to, from, and within buildings. RFI, which is the subset of EMI that occurs in the radio frequency (RF) portion of the electromagnetic (EM) spectrum, can be caused by anything that creates radio waves. Fluorescent lighting is one of the main causes of RFI within buildings today. So, does that mean we need to rip out all the fluorescent lighting? That's one choice, but we could also just use shielded cabling where fluorescent lighting could cause a problem. If you take a break from your reading, climb up into your office's dropped ceiling, and look around, you would probably see wires bundled and tied up to the *true* ceiling. If your office is using fluorescent lighting, the power and data lines should not be running over, or on top of, the fluorescent lights. This is because the radio frequencies being given off can interfere with the data or power current as it travels through these wires. Now, get back down from the ceiling. We have work to do.

Interference interrupts the flow of an electrical current, and fluctuations can actually deliver a different level of voltage than what was expected. Each fluctuation can be

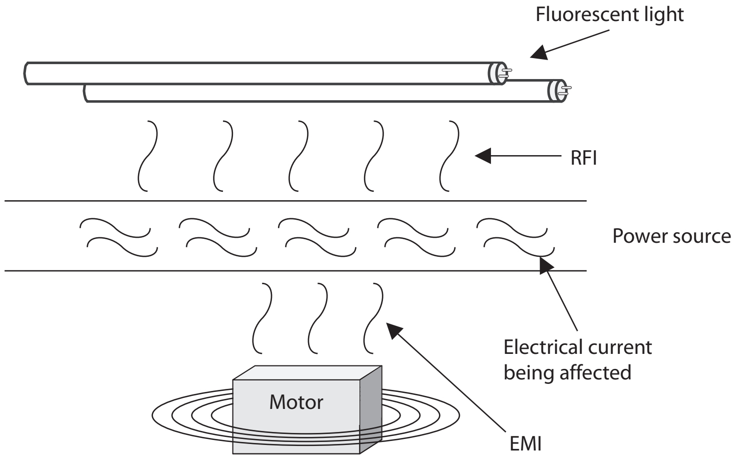


Figure 10-7 RFI and EMI can cause line noise on power lines.

damaging to devices and people. The following explains the different types of voltage fluctuations possible with electric power:

Power excess:

- **Spike** Momentary high voltage
- **Surge** Prolonged high voltage

Power loss:

- **Fault** Momentary power outage
- **Blackout** Prolonged, complete loss of electric power

Power degradation:

- **Sag/dip** Momentary low-voltage condition, from one cycle to a few seconds
- **Brownout** Prolonged power supply that is below normal voltage
- **In-rush current** Initial surge of current required to start a load

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

Because these and other occurrences are common, mechanisms should be in place to detect unwanted power fluctuations and protect the integrity of your data processing environment. *Voltage regulators* and *line conditioners* can be used to ensure a clean and smooth distribution of power. The primary power runs through a regulator or conditioner. They have the capability to absorb extra current if there is a spike and to store energy to add current to the line if there is a sag. The goal is to keep the current flowing at a nice, steady level so neither motherboard components nor employees get fried.

Many data centers are constructed to take power-sensitive equipment into consideration. Because surges, sags, brownouts, blackouts, and voltage spikes frequently cause data corruption, the centers are built to provide a high level of protection against these events. Other types of environments usually are not built with these things in mind and do not provide this level of protection. Offices usually have different types of devices connected and plugged into the same outlets. Outlet strips are plugged into outlet strips, which are connected to extension cords. This causes more line noise and a reduction of voltage to each device. Figure 10-8 depicts an environment that can cause line noise, voltage problems, and possibly a fire hazard.

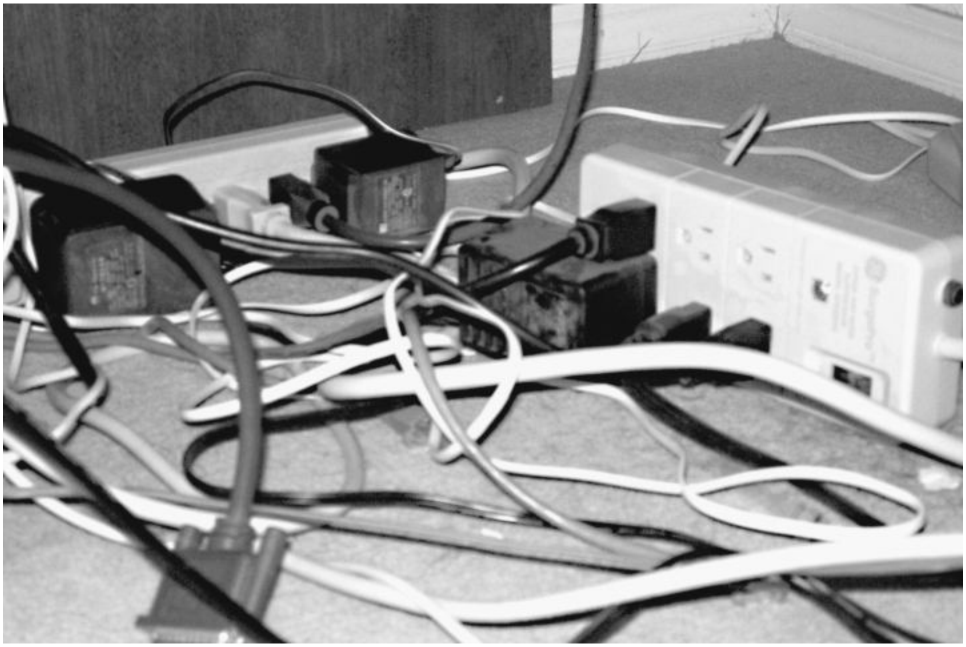


Figure 10-8 This configuration can cause a lot of line noise and poses a fire hazard.

Power Protection Protecting power can be done in three ways: through online UPSs, through standby UPSs, and through the power line conditioners discussed in the previous section. UPSs use battery packs that range in size and capacity. *Online UPS systems* use AC line voltage to charge a bank of batteries. When in use, the UPS has an inverter that changes the DC output from the batteries into the required AC form and regulates the voltage as it powers computer devices. This conversion process is shown in Figure 10-9.

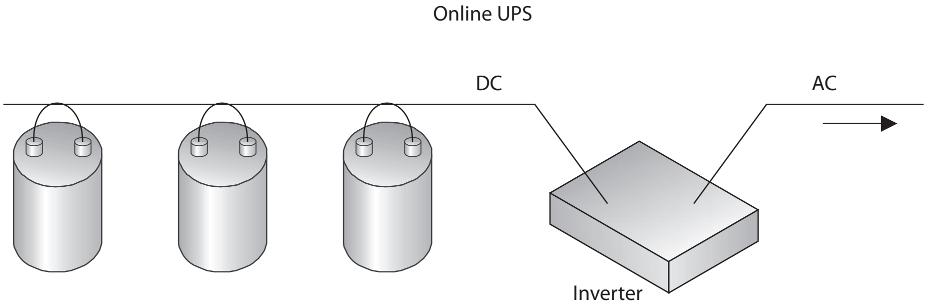


Figure 10-9 A UPS device converts DC current from its internal or external batteries to usable AC by using an inverter.

Online UPS systems have the normal primary power passing through them day in and day out. They constantly provide power from their own inverters, even when the electric power is in proper use. Since the environment's electricity passes through this type of UPS all the time, the UPS device is able to quickly detect when a power failure takes place. An online UPS can provide the necessary electricity and picks up the load after a power failure much more quickly than a standby UPS.

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

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

Heating, Ventilation, and Air Conditioning

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

Most electronic equipment must operate in a climate-controlled atmosphere. Although it is important to keep the atmosphere at a proper working temperature, you must also be aware that the components within the equipment can suffer from overheating even in a climate-controlled atmosphere if the internal computer fans are not cleaned or are blocked. When devices are overheated, the components can expand and contract, which causes components to change their electronic characteristics, reducing their effectiveness or damaging the system overall.

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

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

Lower temperatures can cause mechanisms to slow or stop, and higher temperatures can cause devices to use too much fan power and eventually shut down. Table 10-1 lists different components and their corresponding damaging temperature levels.

Table 10-1 Components Affected by Specific Temperatures

Material or Component	Damaging Temperature
Computer systems and peripheral devices	175°F
Magnetic storage devices	100°F
Paper products	350°F

Fire Safety

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

Fire detection response systems come in many different forms. Manual detection response systems are the red pull boxes you see on many building walls. Automatic detection response systems have sensors that react when they detect the presence of fire or smoke. We will review different types of detection systems in the next section.

Fire suppression is the use of a suppression agent to put out a fire. Fire suppression can take place manually through handheld portable extinguishers or through automated systems such as water sprinkler systems or CO_2 discharge systems. The upcoming "Fire Suppression" section reviews the different types of suppression agents and where they are best used. Automatic sprinkler systems are widely used and highly effective in protecting buildings and their contents. When deciding upon the type of fire suppression systems to install, an organization needs to evaluate many factors, including an estimate of the occurrence rate of a possible fire, the amount of damage that could result, the types of fires that would most likely take place, and the types of suppression systems to choose from.

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

Types of Fire Detection

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

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

There are six classes (A, B, C, D, E, and F) of fire, which are explained in the "Fire Suppression" section. You need to know the differences between the types of fire so you know how to properly extinguish each type. Portable fire extinguishers have markings that indicate what type of fire they should be used on, as illustrated in Figure 10-10. The markings denote what types of chemicals are within the canisters and what types of fires they have been approved to be used on. Portable fire extinguishers should be located within 50 feet of any electrical equipment and also near exits. The extinguishers should be marked clearly, with an unobstructed view. They should be easily reachable and operational by employees and inspected quarterly.

A lot of computer systems are made of components that are not combustible but that will melt or char if overheated. Most computer circuits use only 2 to 5 volts of direct current, which usually cannot start a fire. If a fire does happen in a server room, it will most likely be an electrical fire caused by overheating of wire insulation or by overheating components that ignite surrounding plastics. Prolonged smoke usually occurs before combustion.

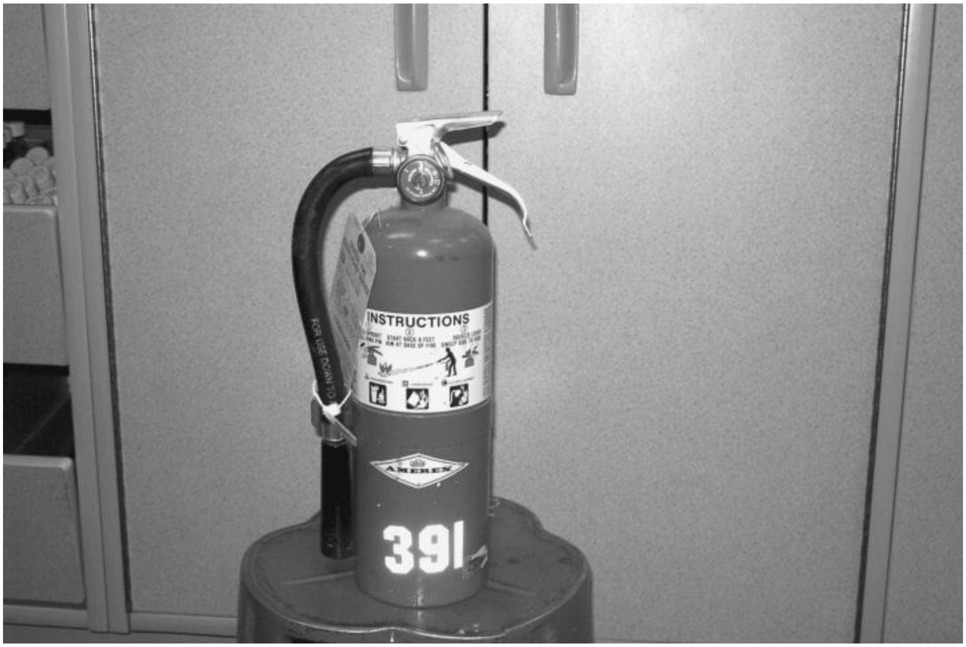


Figure 10-10 Portable extinguishers are marked to indicate what type of fire they should be used on.

Fire Resistance Ratings

Fire resistance ratings are the result of tests carried out in laboratories using specific configurations of environmental settings. ASTM International is the organization that creates the standards that dictate how these tests should be performed and how to properly interpret the test results. ASTM International accredited testing centers carry out the evaluations in accordance with these standards and assign fire resistance ratings that are then used in federal and state fire codes. The tests evaluate the fire resistance of different types of materials in various environmental configurations. Fire resistance represents the ability of a laboratory-constructed assembly to contain a fire for a specific period. For example, a 5/8-inch-thick drywall sheet installed on each side of a wood stud provides a one-hour rating. If the thickness of this drywall is doubled, then this would be given a two-hour rating. The rating system is used to classify different building components.

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

Smoke Activated Smoke-activated detectors are good for early warning devices. They can be used to sound a warning alarm before the suppression system activates. A photoelectric device, also referred to as an optical detector, detects the variation in light intensity. The detector produces a beam of light across a protected area, and if the beam is obstructed, the alarm sounds. Figure 10-11 illustrates how a photoelectric device works.

Another type of photoelectric device samples the surrounding air by drawing air into a pipe. If the light source is obscured, the alarm will sound.

Heat Activated Heat-activated detectors can be configured to sound an alarm either when a predefined temperature (fixed temperature) is reached or when the temperature increases over time (rate of rise). Rate-of-rise temperature sensors usually provide a quicker warning than fixed-temperature sensors because they are more sensitive, but they

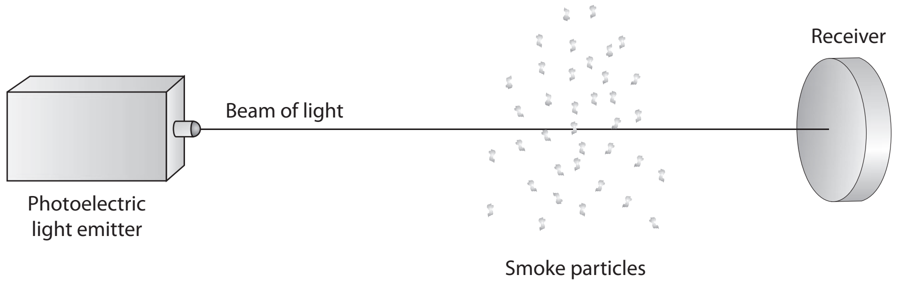


Figure 10-11 A photoelectric device uses a light emitter and a receiver.

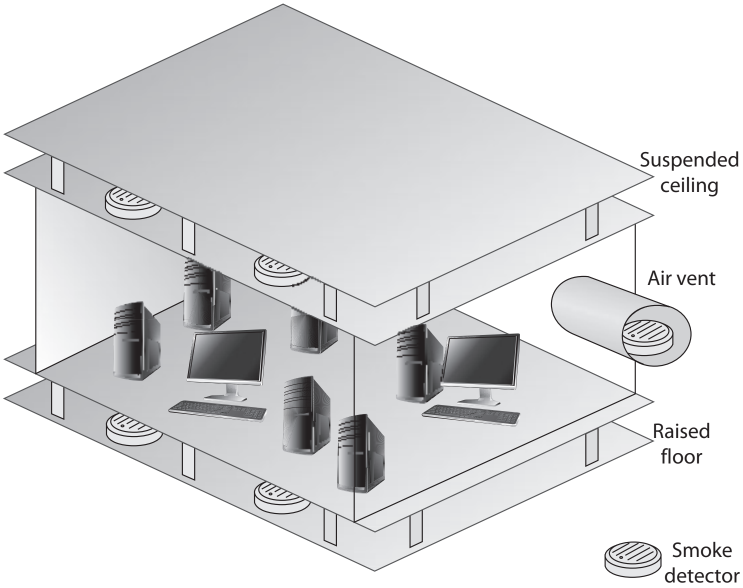


Figure 10-12 Smoke detectors should be located above suspended ceilings, below raised floors, and in air vents.

can also cause more false alarms. The sensors can either be spaced uniformly throughout a facility or implemented in a line type of installation, which is operated by a heat-sensitive cable.

It is not enough to have these fire and smoke detectors installed in a facility; they must be installed in the right places. Detectors should be installed both on and above suspended ceilings and raised floors because organizations run many types of wires in both places that could start an electrical fire. No one would know about the fire until it broke through the floor or dropped ceiling if detectors were not placed in these areas. Detectors should also be located in enclosures and air ducts because smoke can gather in these areas before entering other spaces. It is important that people are alerted about a fire as quickly as possible so damage may be reduced, fire suppression activities may start quickly, and lives may be saved. Figure 10-12 illustrates the proper placement of smoke detectors.

Fire Suppression

It is important to know the different types of fire and what should be done to properly suppress each type. Each fire type has a class that indicates what materials are burning and how to suppress the fire. Unfortunately, three slightly different classifications are in use around the world today (United States, European Union, and Australia). Table 10-2 shows the EU classification fires and their suppression agents. We show this classification because it provides the most granularity. More important than memorizing the letter assigned to each class is to know which suppression methods work best for the different types of fire.

EU Fire Class	Type of Fire	Elements of Fire	Suppression Agent
A	Common combustibles	Wood products, paper, and laminates	Water, foam, dry powders, wet chemicals
B	Liquid	Petroleum products and coolants	CO_2, foam, dry powders
C	Gases	Butane, propane, or methane	Dry powders
D	Combustible metals	Aluminum, lithium, or magnesium	Dry powders
E	Electrical	Electrical equipment and wires	CO_2, dry powders
F	Cooking oils and fats	Typically found in food preparation and storage areas	Wet chemicals

Table 10-2 Six EU Types of Fires and Their Suppression Methods

At the risk of confusing things, we also list here the U.S. classification of fires for reference.

U.S. Class	Type of Fire
A	Common combustibles (same as EU)
B	Liquids and gases (EU Classes B and C combined)
C	Electrical (EU Class E)
D	Metals (same as EU)
K	Cooking oils and fats (EU Class F)

You can suppress a fire in several ways, all of which require taking certain precautions. A fire suppression agent is the substance used to extinguish it. The agent can be delivered in a variety of ways such as a portable fire extinguisher or an overhead distribution system (e.g., water sprinklers). When designing and implementing fire controls, it is critical to match the right suppression agent with the specific facility we're trying to protect. Overhead water sprinklers may be fine for regular work areas but would be catastrophic in a data center. Gases, such as CO_2 will reduce damage to our data assets but could suffocate humans in confined spaces. If you use CO_2, the suppression-releasing device should have a delay mechanism within it that makes sure the agent does not start applying CO_2 to the area until after an audible alarm has sounded and people have been given time to evacuate. CO_2 is a colorless, odorless substance that is potentially lethal because it removes oxygen from the air. Gas masks do not provide protection against CO_2. This type of fire suppression mechanism is best used in unattended facilities and areas.

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

Combustion Element	Suppression Agent	How Suppression Works
Fuel	Soda acid	Removes fuel
Oxygen	Carbon dioxide	Displaces oxygen
Temperature	Water	Reduces temperature
Chemical reaction	FM-200 (Halon substitute)	Interferes with the chemical reactions between elements

Table 10-3 How Different Substances Interfere with Elements of Fire

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

Wet chemical fire extinguishers contain a potassium solution that cools the fire. However, they have an added benefit of chemically reacting with hot oil or fat, creating a soapy film on the surface of these fuels, which starves the fire. For this reason, wet chemical extinguishers are the preferred way of putting out fires involving cooking oils and fats. These extinguishers are also useful for putting put out Class A fires.

A fire needs fuel, oxygen, and high temperatures to sustain its chemical reactions. Fire suppression approaches target one of these three required elements, or the chemical reaction itself. Table 10-3 shows how different suppression substances interfere with these elements of fire.

The HVAC system should be connected to the fire alarm and suppression system so that it properly shuts down if a fire is identified. A fire needs oxygen, and this type of system can feed oxygen to the fire. Plus, the HVAC system can spread deadly smoke into all areas of the building. Many fire systems can configure the HVAC system to shut down if a fire alarm is triggered.

Water Sprinklers

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

Plenum Area

Wiring and cables are strung through *plenum areas*, such as the space above dropped ceilings, the space in wall cavities, and the space under raised floors. Plenum areas should have fire detectors. Also, only plenum-rated cabling should be used in plenum areas, which is cabling that is made out of material that does not release hazardous gases if it burns.