LESSON 1 : Understanding Security Layers

OBJECTIVE DOMAIN MATRIX

SKILLS/CONCEPTS	MTA EXAM OBJECTIVE	MTA EXAM OBJECTIVE NUMBER
Introducing Security	Understand core security principles.	1.1
Looking at Physical Security as the First Line of Defense	Understand physical security.	1.2

KEY TERMS

access control
attack surface
availability
confidentiality
defense in depth
flash drive
integrity
keylogger
mobile device
principle of least privilege
removable device
residual risk
risk
risk acceptance
risk assessment
risk avoidance
risk management
risk mitigation
risk transfer
social engineering
threat

When you think about security, you can start by thinking about your stuff. We all have stuff. We have stuff that we really care about, stuff that would be difficult to replace, and stuff that has great sentimental value. We have stuff we don't want other people to find out about. We even have stuff that we could probably live without. Now think about where you keep your stuff. It could be in your house, car, school, or office; in a locker, backpack, or suitcase; or in a number of other places. Think about all of the bad things that could happen to your stuff. You could be robbed, or you could experience a disaster such as a fire, earthquake, or flood. In any case, you want to protect your possessions—no matter where the threat comes from.
At a high level, security is about protecting stuff. In the case of your personal stuff, it's about making sure you lock the door when you leave the house; remembering to take your purse with you when you leave a

restaurant; or even making sure you hide all the presents you bought for the holidays in the back of your car before you head back into the mall.

Many of the security topics we discuss in this lesson boil down to the same common sense you use every day to protect your stuff. In the business environment, however, the stuff we're protecting is assets, information, systems, and networks, and we can protect these valuables with a variety of tools and techniques that we discuss at length in this book.
In this lesson, we start with the basics. We'll look at some of the underlying principles of a security program to set the foundation for your understanding of the more advanced topics covered later in the book. We'll also discuss the concept of physical security, which is critical not only for securing physical assets, but for securing information assets as well. By the time we're done, you'll have a good idea how to protect stuff for a living.

Introducing Security

THE BOTTOM LINE
Before you can start securing your environment, you need to have a fundamental understanding of the standard concepts of security. It's easy to start buying firewalls, but until you understand what you're trying to protect, why it needs to be protected, and what you're protecting it from, you're just throwing your money away.

When you are working in the information security field, one of the first acronyms you will encounter is CIA—but don't confuse this with the government agency with the same acronym. Rather, in this context, CIA represents the core goals of an information security program:

- Confidentiality
- Integrity

CERTIFICATION READY
Can you list and describe what CIA stands for as it relates to security?
1.1

- Availability

Understanding Confidentiality

Confidentiality is a concept we deal with frequently in real life. For instance, we expect our doctors to keep our medical records confidential, and we trust our friends to keep our secrets confidential. In the business world, we define confidentiality as the characteristic of a resource ensuring access is restricted to only permitted users,

applications, or computer systems. But what does this mean in reality? In short, confidentiality deals with keeping information, networks, and systems secure from unauthorized access.

Confidentiality is particularly critical in today's environment. Lately, in a few high-profile instances, several large companies have leaked people's personal information. These breaches in confidentiality made the news largely because the leaked information could be used to perpetrate identity theft against the people whose information was disseminated.

There are several technologies that support confidentiality in an enterprise security implementation. These include:

- Strong encryption
- Strong authentication
- Stringent access controls

Another key component to consider when discussing confidentiality is how to determine what information is considered confidential. Some common classifications of data are "Public," "Internal Use Only," "Confidential," and "Strictly Confidential." You will also see the classification "Privileged" used frequently in the legal profession. Similarly, the military

> **XREF**
> Lesson 2 contains more details on strong encryption, strong authentication, and stringent access controls.

often categorizes information as "Unclassified," "Restricted," "Confidential," "Secret," or "Top Secret." These classifications are then used to determine what measures are appropriate to protect the information. If your information is not classified, you are left with two options—you can either protect all your information as if it were confidential (an expensive and daunting task), or you can treat all your information as if it were "Public" or "Internal Use Only" and not take stringent protection measures.

> **TAKE NOTE***
> Classify your data and assets—it's the only way you can effectively protect them.

Understanding Integrity

In the information security context, ***integrity*** is defined as the consistency, accuracy, and validity of data or information. One of the goals of a successful information security program is to ensure that data is protected against any unauthorized or accidental changes. Therefore, a security program should include processes and procedures to manage intentional changes, as well as the ability to detect changes. Some of the many processes that can be used to effectively ensure the integrity of information include authentication, authorization, and accounting. For example, you could use rights and permissions to control who can access certain information or resources. You can also use a hashing function (a mathematical function) that can be calculated on data or a message before and after a designated period of time to show whether information has been modified during the specified time. You could also use an auditing or accounting system that records when changes have been made.

Understanding Availability

Availability is the third core security principle, and it describes a resource being accessible to a user, application, or computer system when required. In other words, availability means that when a user needs to get to information, he or she has the ability to do so.
Typically, threats to availability come in two types: accidental and deliberate. Accidental threats include natural disasters like storms, floods, fire, power outages, earthquakes, and so forth. This category also includes outages due to equipment failure, software problems, and other unplanned system, network, or user issues. The second category—deliberate threats—is related to outages that result from the exploitation of a system vulnerability. Some examples of this type of threat include denial of service attacks or network worms that impact vulnerable systems and their availability. In some cases, one of the first actions you will need to take following an outage is determining which category the outage fits into. Companies handle accidental outages very differently than deliberate ones.

Defining Threats and Risk Management

Risk management is the process of identifying, assessing, and prioritizing threats and risks. A ***risk*** is generally defined as the probability that an event will occur. In reality, businesses are only concerned about risks that would negatively impact the computing environment. For instance, there is a risk that you might win the lottery on Friday—but that's not a risk your company is going to actively address, because it would be something positive. Rather, your company would be more concerned with the specific type of risk known as a ***threat***, which is defined as an action or occurrence that could result in the breach, outage, or corruption of a system by exploiting known or unknown vulnerabilities. Typically, when people refer to risk management, they are focusing on this type of negative risk.

The goal of any risk management plan is to remove risks when possible and to minimize the consequences of risks that cannot be eliminated. The first step in creating a risk management plan is to conduct a ***risk assessment***. Risk assessments are used to identify the risks that might impact your particular environment.

Once you have completed your assessment and identified your risks, you need to evaluate each risk for two factors. First, you need to determine the likelihood that a risk will occur in your environment. For example, a tornado is much more likely in Oklahoma than in Vermont. A meteor strike is probably not very likely anywhere, although it's one example commonly used to represent the complete loss of a facility when discussing risk. After you have determined the likelihood of a specific risk, you then need to determine the impact of that risk on your environment. For instance, a virus on a user's workstation generally has a relatively low impact on the company (although a high impact on the user.) A virus on your financial system has a much higher overall impact, although hopefully a lower likelihood.

Once you have evaluated your risks, it's time to prioritize them. One of the best mechanisms to assist with prioritization is to create a risk matrix, which can be used to determine an overall risk ranking. A risk matrix should include the following elements:

TAKE NOTE*
In a mature risk assessment environment,it is common to record your risks in a risk register, which providesa formal mechanism for documenting the risks, impacts, controls, and other information required by the risk management program.

- The risk
- The likelihood that the risk will actually occur
- The impact of the risk

- A total risk score
- The relevant business owner (individual, team or department) for the risk
- The core security principles affected by the risk—confidentiality, integrity, and/or availability
- The appropriate strategy or strategies to deal with the risk

Some additional fields that may prove useful in your risk register are as follows:

- A deliverable date for the risk to be addressed
- Documentation about the residual risk (i.e., the risk that remains after measures have been taken to reduce the likelihood or minimize the effect of an event)
- The status of the strategy or strategies being used to address the risk; this can include indicators like “Planning,” “Awaiting Approval,” “Implementation,” and “Complete”

One easy way to calculate a total risk score is to assign numeric values to your likelihood and impact. For example, you can rank likelihood and impact on a scale from 1 to 5, where 1 equals low likelihood or low probability and 5 equals high likelihood or high impact. You can then multiply the likelihood and impact together to generate a total risk score. By sorting from high to low, you have an easy method to initially prioritize your risks. You should then review the specific risks to determine the final order in which you want to address them. At this point, you may find that external factors, like cost or available resources, affect your priorities.

After you have prioritized your risks, you are ready to choose from among the four generally accepted responses to these risks. They include:

- Avoidance
- Acceptance
- Mitigation
- Transfer

Risk avoidance is the process of eliminating a risk by choosing not to engage in an action or activity. As an example of risk avoidance, consider a person who understands that there is a risk that the value of a stock might drop, so he or she avoids the risk by not purchasing the stock. One problem with risk avoidance is that there is frequently a reward associated with a risk—so if you avoid the risk, you also avoid the reward. For instance, if the stock in the example were to triple in price, the risk-averse investor would lose out on the reward because he or she wanted to avoid the risk.

Risk acceptance is the act of identifying and then making an informed decision to accept the likelihood and impact of a specific risk. To reuse the stock example, risk acceptance is the process in which a buyer thoroughly

researches a company whose stock he or she is interested in, and after considering this information, makes the decision to accept the risk that the stock price might drop.

Risk mitigation consists of taking steps to reduce the likelihood or impact of a risk. A common example of risk mitigation is the use of redundant hard drives in a server. There is a risk of hard drive failure in any system. By using redundant drive architecture, you can mitigate the risk of a drive failure by having the redundant drive. In other words, although the risk still exists, it has been reduced by your actions.

Risk transfer is the act of taking steps to move responsibility for a risk to a third party through insurance or outsourcing. For example, there is a risk that you may have an accident while driving your car. You transfer this risk by purchasing insurance so that in the event of an accident, your insurance company is responsible for paying the majority of the associated costs.

As mentioned earlier, one other important concept in risk management is that of ***residual risk***. Residual risk is the risk that remains after measures have been taken to reduce the likelihood or minimize the effect of a particular event. To continue with the car insurance example, your residual risk in the event of an accident would be the deductible you have to pay before your insurance company assumes responsibility for the remainder of the damage.

> **TAKE NOTE***
> There are many different ways to identify, assess, and prioritize risks. There is no one right way. Use the techniques that best fit your environment and requirements.

Now, as part of our discussion of risk, we also need to look at two final concepts that will help you understand the foundations of security principles and risk management: the principle of least privilege and the idea of an attack surface.

Understanding the Principle of Least Privilege

The ***principle of least privilege*** is a security discipline that requires that a particular user, system, or application be given no more privilege than necessary to perform its function or job. This sounds like a very commonsense approach to assigning permissions, and when seen on paper, it is. However, when you start to apply this principle in a complex production environment, it becomes significantly more challenging.

The principle of least privilege has been a staple in the security arena for a number of years, and many organizations have struggled to implement it successfully. However, with today's increased focus on security from both a business and a regulatory perspective, organizations are working harder than ever before to build their models around this principle. The regulatory requirements of Sarbanes-Oxley, HIPAA, HITECH, and various state regulations, coupled with organizations' increased focus on the security practices of their business partners, vendors, and consultants, are driving companies to invest in tools, processes, and other resources to ensure this principle is followed.

But why is a principle that sounds so simple on paper so difficult to implement in reality? The challenge is largely related to the complexity of the typical work environment. It is easy to visualize application of the principle of least privilege for a single employee. On a physical basis, the employee needs access to the building he or she works in, any common areas, and his or her office. Logically, the employee also needs to be able to log in to his or her computer, have access to some centralized applications, and have access to a file server, a printer, and an internal web site. Now, imagine that single user multiplied by a thousand—and imagine that these thousand employees work in six different office locations. Some employees need access to all six locations, whereas others only need access to their own location. Still others need access to specific subsets of the six locations; for example, they might need

access to the two offices in their region, or they might require access to the data center so they can provide IT support.

In this situation, instead of a single set of access requirements, you now have multiple departments with varying application requirements. You also have different user types, varying from “regular” users to power users to administrators; therefore, you need to determine not only what type of user each employee is, but also which internal applications he or she can access. Add to this mix new hires, employees who are transferred or promoted, and employees who leave the company, and you can start to see how making sure each employee has the minimum amount of access required to do his or her job can be a time-intensive activity.

But wait—we’re not done. In addition to physical and user permissions, you also need to be aware that in many IT environments, certain applications require access to data and/or other applications. Thus, to follow the principle of least privilege, you must ensure that these applications have the minimum necessary access in order to function properly. This can be extremely difficult when working in a Microsoft Active Directory environment, due to the detailed permissions included in Active Directory. Determining which permissions an application requires to function properly with Active Directory can be challenging in the extreme.

To further complicate matters, in industries where there is heavy regulation, like the financial or medical fields, or when regulations like Sarbanes-Oxley are in effect, there are additional requirements stating that you must audit regularly to ensure you have successfully implemented and validated privileges across the enterprise.

A detailed discussion of how to implement and maintain the principle of least privilege is beyond the scope of this book, but there are some high-level tools and strategies you should be aware of, including the following:

- **Groups:** Groups allow you to logically group users and applications so that permissions are not applied on a user-by-user or application-by-application basis.
- **Multiple user accounts for administrators:** Administrators are one of the biggest challenges when implementing the principle of least privilege. Administrators are typically also users, and it is seldom a good idea for administrators to perform their daily user tasks as an administrator. To address this issue, many companies issue their administrators two accounts—one for their role as a user of the company’s applications and systems and the other for their role as an administrator.
- **Account standardization:** The best way to simplify a complex environment is to standardize a limited number of account types. Each different account type permitted in your environment adds an order of magnitude to your permissions management strategy. By standardizing a limited set of account types, you make your job much easier.
- **Third-party applications:** A variety of third-party tools have been designed to make managing permissions easier. These range from account life-cycle management applications to auditing applications to application firewalls.
- **Processes and procedures:** One of the easiest ways to manage permissions in your environment is to have a solid framework of processes and procedures for managing accounts. With this framework to rely on, you don’t have to address each account as a

unique circumstance. Rather, you can rely on the defined process to determine how all accounts are created, classified, permissioned, and maintained.

> **TAKE NOTE***
> Perfect implementation of the principle of least privilege is very rare.
> A best effort is typically what is expected and what is achievable.

Understanding Attack Surface

One final concept to tackle when evaluating the security of your environment is that of an ***attack surface***. With respect to systems, networks, and applications, this is another idea that has been around for quite some time. An attack surface consists of the set of methods and avenues an attacker can use to enter a system and potentially cause damage. The larger the attack surface of a particular environment, the greater the risk of a successful attack.

To calculate the attack surface of an environment, it's frequently easiest to divide the evaluation into three components:

- Application
- Network
- Employee

When evaluating the *application attack surface*, you need to look at things like:

- The amount of code in an application
- The number of data inputs to an application
- The number of running services
- Which ports the application is listening on

Similarly, when evaluating the *network attack surface*, you should consider the following:

- Overall network design
- Placement of critical systems
- Placement and rule sets on firewalls
- Other security-related network devices, such as IDS, VPN, and so on

Finally, when evaluating the *employee attack surface*, you should consider the following factors:

- The risk of social engineering
- The potential for human errors
- The risk of malicious behavior

Once you have evaluated these three types of attack surfaces, you will have a solid understanding of the total attack surface presented by your environment, as well as how an attacker might try to compromise your environment.

Understanding Social Engineering

As previously mentioned, one of the key factors to consider when evaluating the employee attack surface is the risk of a social engineering attack. ***Social engineering*** is a method used to gain access to data, systems, or networks, primarily through misrepresentation. This technique typically relies on the trusting nature of the person being attacked.

In a typical social engineering attack, the attacker will try to appear as harmless or respectful as possible. These attacks can be perpetrated in person, through email, or via phone. Attackers will try techniques ranging from pretending to be a help desk or support department staffer, claiming to be a new employee, or in some cases, even offering credentials that identify them as an employee of the company.

Generally, these attackers will ask a number of questions in an attempt to identify possible avenues to exploit during an attack. If they do not receive sufficient information from one employee, they may reach out to several others until they have sufficient information for the next phase of an attack.

To avoid social engineering attacks, remember the following techniques:

- **Be suspicious:** Phone calls, emails, or visitors who ask questions about the company, its employees, or other internal information should be treated with extreme suspicion, and if appropriate, reported to security personnel.
- **Verify identity:** If you receive inquiries that you are unsure of, verify the identity of the requestor. If a caller is asking questions that seem odd, try to get his or her number so you can call back. Then, verify that the phone number you have been given is from a legitimate source. Similarly, if someone approaches you with a business card as identification, ask to see a picture ID. Business cards are easy to print, and they are even easier to take from the “Win a Free Lunch” bowl at a local restaurant.
- **Be cautious:** Do not provide sensitive information unless you are certain not only of the person’s identity, but also his or her right to have the information.
- **Don’t use email:** Email is inherently insecure and prone to a variety of address spoofing

techniques. Therefore, don't reveal personal or financial information via email. Never respond to email requests for sensitive information—and be especially cautious of providing this information after following web links embedded in email. A common trick is to embed a survey link in an email, possibly offering a prize or prize drawing, and then asking questions about the computing environment like "How many firewalls do you have deployed?" or "What firewall vendor do you use?" Employees are so accustomed to seeing these types of survey requests in their inboxes that they seldom think twice about responding to them.

Linking Cost with Security

> **TAKE NOTE***
> The key to thwarting a social engineering attack is employee awareness.
> If your employees know what to watch for, an attacker will find little success.

There are some points that you should keep in mind when developing a security plan. First, security costs money. Typically, the more money you spend, the more secure your information or resources will be (up to a point). So, when looking at risk and threats, you need to consider how valuable certain confidential data or resources are to your organization and also how much money you are willing to spend to protect those data or resources.

In addition to considering cost, you should also strive to make the security measures as seamless as possible to authorized users who are accessing the confidential information or resource. If security becomes a heavy burden, users will often look for methods to circumvent the measures you have established. Of course, training goes a long way in protecting your confidential information and resources because it shows users what warning signs to watch for.

Looking at Physical Security as the First Line of Defense

> **THE BOTTOM LINE**
> There are a number of factors to consider when designing, implementing, or reviewing physical security measures taken to protect assets, systems, networks, and information. These include understanding site security and computer security; securing removable devices and drives; access control; mobile device security; disabling the Log On Locally capability; and identifying and removing keyloggers.

Most businesses exercise some level of control over who is able to access their physical environment. When securing computer-related assets and data, there is a tendency to only look at the virtual world, paying little attention to the issue of physical security. However, if you work for a large company in a location with a data center, you may see badge readers and/or keypads to access the building and any secure areas, along with guards and perhaps even logbooks to control and track the people who enter in the building. Office keys and desk drawer keys provide yet another layer of security. In smaller offices, similar measures may be in place, albeit on a smaller scale.

> **CERTIFICATION READY**
> Why is physical security so important to a server even when you need usernames and passwords to access that server?
> 1.2

> **TAKE NOTE***
> If someone can get physical access to a server where confidential data is stored, with the right tools and enough time, that person can bypass any security the server uses to protect the data.

This multilayered approach to physical security is known as defense in depth or a layered security approach. See Figure 1-1. Securing a physical site is more than just putting a lock on the front door and making sure you use that lock. Rather, it is a complex challenge for any security professional.

> **TAKE NOTE***
> Security does not end with physical security. You also need to look at protecting confidential information with technology based on authentication, authorization, and accounting—including use of rights, permissions, and encryption.

Understanding Site Security

> Site security is a specialized area of the security discipline. This section is meant to introduce you to some of the more common concepts and technologies you may encounter when working in the site security field.

UNDERSTANDING ACCESS CONTROL

Before we jump into site security details, you must first understand what is meant by the term “access control.” ***Access control*** is a key concept when thinking about physical security. It is also a little confusing, because you will frequently hear the phrase used when discussing information security. In the context of physical security, access control is the process of restricting access to a resource to only permitted users, applications, or computer systems.

If you think about it, you can probably come up with several everyday examples of access control. For instance, when you close a door and lock it, you are practicing access control. When you use a baby gate to keep a toddler from falling down a staircase, you are practicing access control. Similarly, when you put a fence around your yard to keep your dog out of the neighbor’s flowers, you are practicing access control.

The difference between the access control you practice in your everyday life and the access control you will encounter in the business world is the nature of what you are protecting and the technologies you have available to secure it. We will cover these topics in more detail through the rest of this lesson.

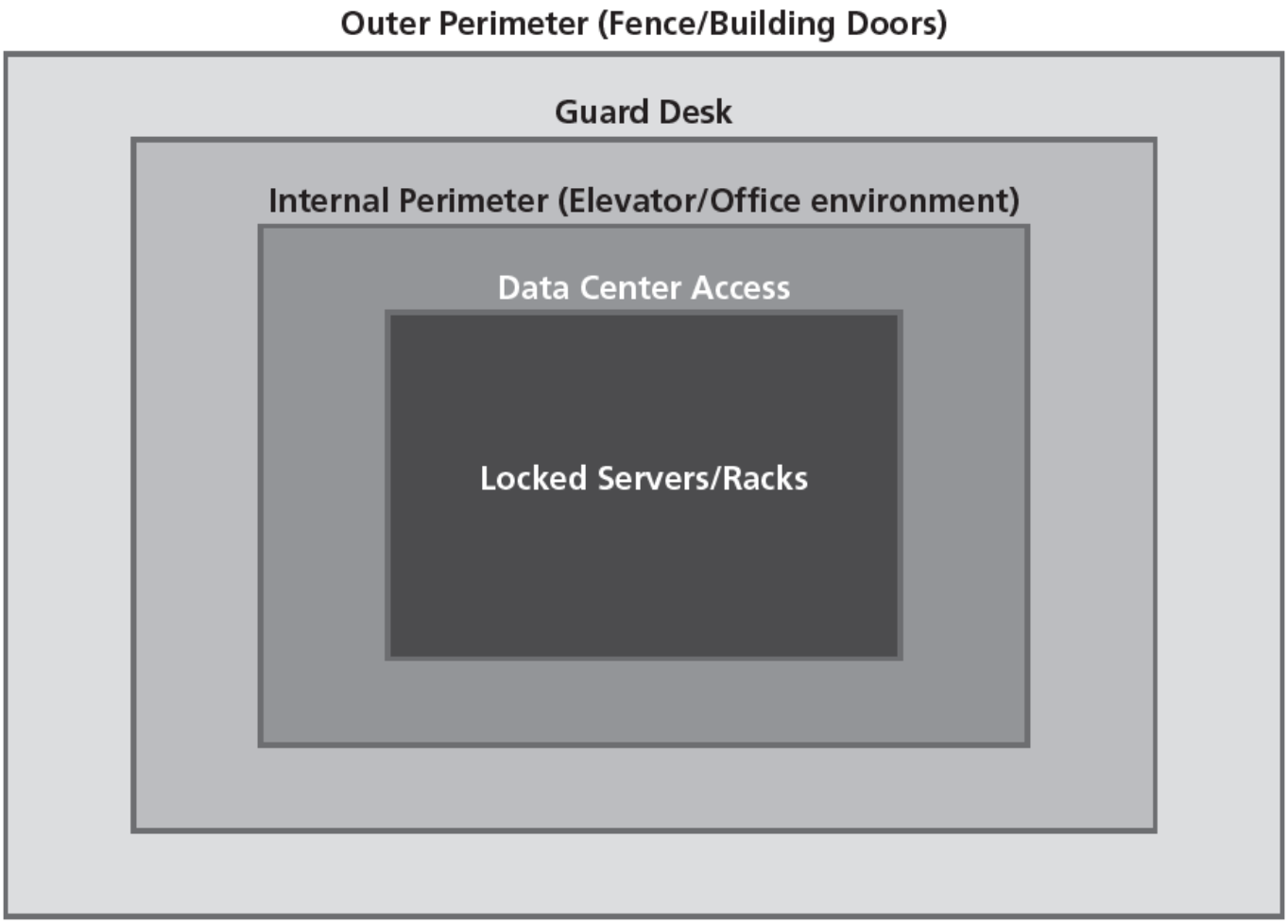

Figure 1-1 Layered site security model

As previously mentioned, site security involves securing the physical premises. One fundamental concept used when designing a security environment is that of defense in depth. ***Defense in depth*** means using multiple layers of security to defend your assets. That way, even if an attacker breaches one layer of your defense, you have additional layers to keep that person out of the critical areas of your environment.

A simple example of defense in depth that you may have encountered in the "real world" is a hotel room that contains a locked suitcase. To get into the locked hotel room, you must get the key to work. After you accomplish this task, there is a deadbolt that must be bypassed. And once you are past the deadbolt, there is still the lock on the suitcase that must be breached. Beyond the idea of defense in depth, there are several other goals to keep in mind when designing a physical security plan:

- **Authentication:** Site security must address the need to identify and authenticate the people who are permitted access to an area.
- **Access control:** Once a person's identity has been proven and authenticated, site security must determine what areas that person has access to.
- **Auditing:** Site security must also provide the ability to audit activities within the facility. This can be done by reviewing camera footage, badge reader logs, visitor registration logs, or other mechanisms.

For the purposes of this lesson, we will break the physical premises into three logical areas:

- **The external perimeter**, which makes up the outermost portion of the location. This typically includes the driveways, parking lots, and any green space the location may support. This does not include things like public roads.
- **The internal perimeter**, which consists of any buildings on the premises. If the location supports multiple tenants, your internal perimeter is restricted to only the buildings you occupy.
- **Secure areas**, which are locations within the building that have additional access restrictions and/or security measures in place. These might include data centers, network rooms, wiring closets, or departments like Research and Development or Human Resources.

UNDERSTANDING EXTERNAL PERIMETER SECURITY

The external security perimeter is the first line of defense surrounding your office. However, security measures in this area probably vary the most of any area we will discuss. For instance, if you are trying to protect a top-secret government installation, your external perimeter security will likely consist of multiple fences, roving guard patrols, land mines, and all sorts of other measures you won't see in the corporate world. On the other hand, if your office is in a multitenant office park, the external perimeter security may consist only of streetlights. Most companies fall somewhere in between. Common security measures you may encounter with respect to an organization's external perimeter include the following:

- Security cameras
- Parking lot lights
- Perimeter fence
- Gate with guard
- Gate with access badge reader
- Guard patrols

One challenge associated with security cameras is that these cameras are only as good as the people monitoring them. Because monitoring cameras is a resource-intensive, expensive undertaking, in most office environments, there isn't anyone actively watching these cameras. Instead, cameras are used after an incident occurs to determine what happened or who is responsible.

> **TAKE NOTE***
> Test your camera's playback capabilitiesregularly. Because cameras are almost always used to review events after the fact, you need to be sure your system is successfully recording the data.

UNDERSTANDING THE INTERNAL PERIMETER

The internal security perimeter starts with the building walls and exterior doors and includes any internal security measures, with the exception of secure areas within the building. Some of the features you may use to secure an internal perimeter include the following:

- Locks (on exterior doors, internal doors, office doors, desks, filing cabinets, etc.)
- Keypads
- Security cameras
- Badge readers (on doors and elevators)
- Guard desks
- Guard patrols
- Smoke detectors
- Turnstiles
- Mantraps

The key security measures implemented in the internal perimeter are those that are used to divide the internal space into discrete segments. This is a physical implementation of the principle of least privilege. For example, if an organization's office includes finance, human resources, and sales departments, it would not be unusual to restrict access to the finance department to only those people who work in finance. You generally don't need human resources staffers wandering around your finance area. These sorts of segregations may be based on floors, areas, or even series of offices, depending on the physical layout.

DEFINING SECURE AREAS

Secure areas within an office would include places like a data center, the research and development department, a lab, a telephone closet, a network room, or any other area that requires additional security controls not only to restrict external attackers, but also to limit internal employee access. Secure area security technologies include the following:

- Badge readers
- Keypads
- Biometric technologies (e.g., fingerprint scanners, retinal scanners, voice recognition systems, etc.)
- Security doors
- X-ray scanners

- Metal detectors
- Cameras
- Intrusion detection systems (light beam, infrared, microwave, and/or ultrasonic)

> **TAKE NOTE***
> Smaller offices that are not occupied at night may take advantage of remote monitoring and intrusion detection systems in their internal perimeter. Larger locations typically have some activities occurring on nights and weekends, which makes use of these technologies more challenging.

UNDERSTANDING SITE SECURITY PROCESSES

Although technology forms a significant component of an organization's physical security, the processes you put in place to support this technology are just as critical. In fact, you should have such processes at all levels of your site.

In the external perimeter, you might have a process to manage entry to the parking lot through a gate, or there may be a process for how often the guards patrol the parking lot. Included in those processes should be how to document findings, track entry and exits, and respond to incidents. For example, your guard tour process should include instructions on how to handle an unlocked car or a suspicious person, or, with the heightened awareness of possible terrorist attacks, how to handle an abandoned package.

In the internal perimeter, you might have processes that include guest sign-in procedures, equipment removal procedures, guard rotations, or when the front door is to be left unlocked. You should probably also have processes to handle deliveries, how/when to escort visitors in the facility, and even what types of equipment may be brought into the building. For example, many companies prohibit bringing personal equipment into the office due to the risk that an employee could use his or her personal laptop to steal valuable company information.

Once you reach the secure area layer, you will generally have procedures for controlling who is permitted to enter the data center and how they will access the data center. In addition, you will have multiple mechanisms to ensure that only authorized people are granted access including locked doors, biometric devices, cameras, and security guards.

> **TAKE NOTE***
> Cameras are available on virtually every cell phone on the market today. If you need to ensure that cameras are not used in your facility, plan on taking phones at the door or disabling their camera function.

Understanding Computer Security

Computer security consists of the processes, procedures, policies, and technologies used to protect computer systems. For the purposes of this lesson, computer security will refer specifically to physically securing computers; other facets of computer security are discussed throughout the rest of the book.

In addition to the many physical security measures already described, there are some additional tools that can be used to secure actual computers. Before we start discussing these tools, however, we first need to differentiate

among three main types of computers:

- **Servers:** These are computers used to run centralized applications and deliver the applications across a network. This can be an internal network (such as for a business) or perhaps even the Internet (for public access). The computer that hosts your favorite website is an excellent example of a server. Servers are typically configured with redundant capabilities, ranging from redundant hard drives to fully clustered servers.
- **Desktop computers:** These computers are usually found in office environments, schools, and homes. Such computers are meant to be used in a single location and to run applications like word processing, spreadsheets, games, and other local programs. They can also be used to interact with centralized applications or to browse websites.
- **Mobile computers:** This category includes laptop, notebook, tablet, and netbook computers. You could even include smartphones. These machines are used for the same types of functions as desktop computers, but they are meant to be used in multiple locations (for example, home and office). Due to their smaller size, mobile computers were once less powerful than desktop computers, but thanks to advances in microprocessor and storage technologies, this gap is rapidly narrowing.

Each type of computer—server, desktop, and mobile—requires different physical security considerations. For example, when securing a server, the first thing you must consider is where the server will be located. Servers are typically much more expensive than desktop or mobile computers and used to run critical applications, so the types of security typically used with servers are largely location based. Servers should be secured in data centers or computer rooms, where you can take advantage of locked doors, cameras, and various other security features described earlier in the lesson.

If you do not have the ability to place a server in a data center or computer room, you should utilize one of the following technologies:

- **Computer security cable:** A cable that is attached to the computer and to a piece of furniture or the wall.
- **Computer security cabinet/rack:** A storage container that is secured with a locking door.

Desktop computers are typically secured with the same types of computer security cables you can use with servers. Desktop computers are frequently used in secure office environments or in people's homes, and they are not particularly expensive relative to other technologies. Accordingly, most companies do not take extraordinary measures to protect the desktop computers in their offices.

Mobile computers, unlike servers and desktops, are highly portable, so there is a unique set of technologies and best practices for protecting these machines from theft or damage. Some of these methods are described in the following section.

UNDERSTANDING MOBILE DEVICE SECURITY

Mobile devices are one of the largest challenges facing many security professionals today. Mobile devices such as laptops, PDAs (personal digital assistants), and smartphones are used to process information, send and receive mail, store enormous amounts of data, surf the Internet, and interact remotely with internal networks and systems. When you consider that you can place a 32 GB MicroSD memory card (see Figure 1-2) in a smartphone that a senior vice president can then use to store all of a company's research and development information, the potential impact to the company should someone steal that phone is staggering. As a result, the industry offers a number of technologies for physically securing mobile devices, including the following:

- **Docking stations:** Virtually all laptop docking stations are equipped with security features. This may involve a key, a padlock, or both, depending on the vendor and model.
- **Laptop security cables:** Used in conjunction with the USS (Universal Security Slot), these cables attach to a laptop and can be wrapped around a secure object like a piece of furniture.
- **Laptop safes:** These are steel safes specifically designed to hold a laptop and be secured to a wall or piece of furniture.
- **Theft recovery software:** These applications enable the tracking of a stolen computer so it can be recovered.
- **Laptop alarms:** These are motion-sensitive alarms that sound in the event that a laptop is moved. Some are also designed in conjunction with a security cable system so that they sound whenever the cable is cut.

> **TAKE NOTE***
> Docking station security only works if you enable it and make sure the docking station is secured to an immovable object. It's frequently just as easy to steal a laptop and its docking station as it is to steal just the laptop.

PDAs and smartphones are typically more difficult to secure than laptops; because they are a new technology that just recently exploded in popularity, only limited security tools are available. For now, you can configure passwords to protect these devices, enable encryption, and remotely wipe phones that are managed by an organization. Some smartphones and PDAs also include GPS components that allow you to track their location.

Of course, there are some best practices (and yes, these are based on common sense) that can be followed when securing both laptops and PDAs or smartphones, including the following:

- **Keep your equipment with you:** Mobile devices should be kept with you whenever possible. This means you should keep your mobile devices on your person or in your hand

luggage when traveling. Similarly, keep your mobile devices in your sight when going through airport checkpoints.

- **Use your trunk:** If you are traveling by car and are unable to take your mobile device with you, lock it in the trunk when you park. Do not leave a mobile device in view in an unattended vehicle, even for a short period of time, and never leave it in a vehicle overnight.
- **Use the safe:** If you are staying in a hotel, lock your mobile device in a safe if one is available.

USING REMOVABLE DEVICES AND DRIVES

In addition to mobile devices, another technology that presents unique challenges to security professionals is removable devices and drives. You can see some examples of common removable devices in Figure 1-2.

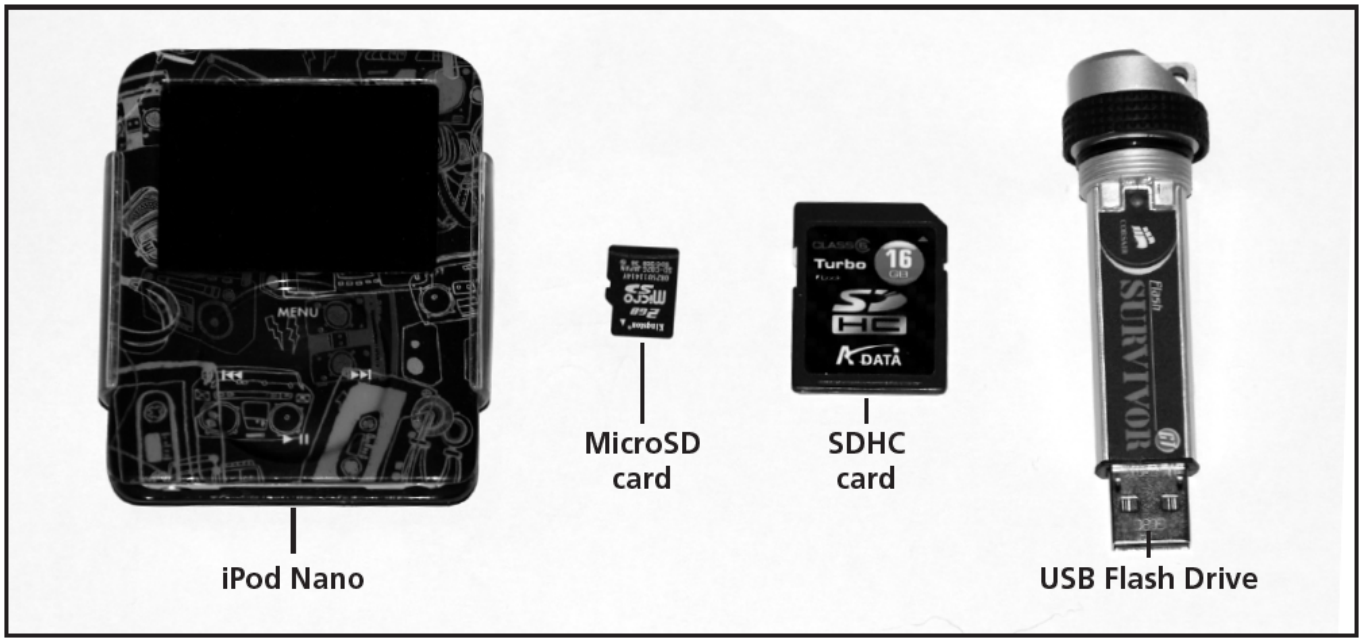

Figure 1-2 Removable devices

A ***removable device*** or drive is a storage device that is designed to be taken out of a computer without turning the computer off. These devices range from the MicroSD memory card, which is the size of your fingernail and can store up to 32 GB of information, to an external hard drive, which can store up to 2 terabytes of data. Floppy disks, CDs, and DVDs are also considered removable drives because they can be used to store critical data.

Removable devices typically connect to a computer through a drive, through external communications ports like USB or Firewire, or, in the case of memory cards, through built-in or USB-based readers. These devices are used for a variety of purposes, including backing up critical data, providing supplemental storage, transferring data between computers, and sometimes even running applications. This form of storage is also used in music players like iPods and Zunes, as well as in personal media players like the Archos and Creative's Zen devices.

There are three basic types of security issues associated with removable storage:

- Loss

- Theft
- Espionage

The loss of a storage device is one of the most common security issues you will encounter. USB drives are especially problematic in this regard. Typically the size of a pack of gum or smaller, these drives are frequently left in conference rooms, in hotel rooms, or in seat pockets on airplanes. Your challenge is how to secure the gigabytes of data that are lost along with these drives. Currently, these devices can be protected with both authentication and encryption. Also, with Windows 7 and Windows Server 2008 R2, Microsoft released BitLocker To Go, which can be used to protect data on mobile storage devices. In addition, some companies may offer their own protection mechanism, such as IronKey. Of course, you need to impress on your users the value of these types of storage. Many users do not give a second thought to throwing a confidential presentation on a ***flash drive*** (a small drive based on flash memory) for a meeting. As part of your awareness efforts, you must educate these users about the value of data, as well as how easy it is to misplace portable storage devices.

Theft is a problem with any portable piece of equipment. Many of the theft-prevention measures discussed with respect to mobile devices apply to removable storage devices as well. For example, keep drives with you whenever possible. When you cannot keep them with you, secure them in a hotel safe, locked desk drawer, or other secure location. Do not leave portable storage out where it can be easily removed from your area. Remember, even though removable devices themselves are relatively inexpensive, the data on them can be irreplaceable, or worse, confidential.

The final area in which these types of devices present a security issue is in conjunction with espionage. Many storage devices come in very small forms, which make them particularly well suited to espionage. For example, you can purchase flash drives disguised as pens, watches, or even as part of a pocketknife. To further compound the problem, everyday technological devices like music players and cell phones often have multiple gigabytes of storage. Even if you manage to ban unauthorized external drives and music players from the work setting, removing employee cell phones is virtually impossible. So, how can you protect your environment from this type of security threat?

> **TAKE NOTE***
> Some workplaces address the issues associated with removable storage by using hardware or software configurations that prohibit their use. Although this can be an effective strategy, it is also expensive and resource intensive.
> Accordingly, there are only a limited number of businesses in which this strategy can be effectively implemented.

The key to this threat is not to try to defend the environment from portable devices, but instead to protect the data from any unauthorized access. This is where the principle of least privilege is critical—if you ensure that employees can only access the data, systems, and networks they need to do their jobs, then you make the task of keeping critical data off portable drives much easier.

> **XREF**
> Encryption is frequently used to secure the data on removable drives.
> This method is discussed in detail in Lesson 2.

UNDERSTANDING KEYLOGGERS

A ***keylogger*** is a physical or logical device used to capture keystrokes. An attacker will either place a device between the keyboard and the computer or install a software program to record each keystroke taken, and then he or she can use software to replay the data and capture critical information like user IDs and passwords, credit card numbers, Social Security numbers, or even confidential emails or other data. There are also wireless keyboard sniffers that can intercept the broadcast keystrokes sent between a wireless keyboard and a computer.

To protect against a physical keylogger, your best tool is visual inspection. Take a look at the connection between the keyboard and the computer. If there is an extra device in between the two, someone is trying to capture your keystrokes. This is especially important when working with shared or public computers, where attackers will utilize keyloggers to cast a wide net and grab whatever critical data someone might enter.

The best defense against a software keylogger is the use of up-to-date antimalware software. Many software keyloggers are identified as malware by these applications. You can also leverage User Account Control and host-based firewalls to prevent a software keylogger from being installed.

To defend against a wireless keyboard sniffer, your best bet is to ensure your wireless keyboard supports encrypted connections. Most current wireless keyboards will either operate in an encrypted mode by default or at least permit you to configure encryption during installation.

> **XREF**
> Lesson 5 contains a more in-depth discussion of antimalware and workstation firewall technologies.

SKILL SUMMARY

IN THIS LESSON YOU LEARNED:

- Before you can start securing your environment, you need to have a fundamental understanding of the standard concepts of security.
- CIA, short for confidentiality, integrity, and availability, represents the core goals of an information security program.
- Confidentiality deals with keeping information, networks, and systems secure from unauthorized access.
- One of the goals of a successful information security program is to ensure integrity, or that information is protected against any unauthorized or accidental changes.
- Availability is defined as the characteristic of a resource being accessible to a user, application, or computer system when required.
- Threat and risk management is the process of identifying, assessing, and prioritizing

threats and risks.

- A risk is generally defined as the probability that an event will occur.
- Once you have prioritized your risks, there are four generally accepted responses to these risks: avoidance, acceptance, mitigation, and transfer.
- The principle of least privilege is a security discipline that requires that a user, system, or application be given no more privilege than necessary to perform its function or job.
- An attack surface consists of the set of methods and avenues an attacker can use to enter a system and potentially cause damage. The larger the attack surface of an environment, the greater the risk of a successful attack.
- The key to thwarting a social engineering attack is employee awareness. If your employees know what to look out for, an attacker will find little success.
- Physical security uses a defense in depth or layered security approach that controls who can physically access an organization's resources.
- Physical premises can be divided into three logical areas: the external perimeter, the internal perimeter, and secure areas.
- Computer security consists of the processes, procedures, policies, and technologies used to protect computer systems.
- Mobile devices and mobile storage devices are among the biggest challenges facing many security professionals today because of their size and portability.
- A keylogger is a physical or logical device used to capture keystrokes.

Knowledge Assessment

Multiple Choice

Circle the letter or letters that correspond to the best answer or answers.

1. Which of the following are valid risk responses? (Choose all that apply.)

a. Mitigation

b. Transfer

c. Investment

d. Avoidance

2. Which of the following are considered removable devices or drives? (Choose all that apply.)

a. iPod

b. Netbook

c. USB flash drive

d. Floppy drive

3. Which of the following would be considered appropriate security measures for a building's external security perimeter? (Choose all that apply.)

a. Motion detector

b. Parking lot lights

c. Turnstile

d. Security guards

4. You are traveling on business and are headed out to dinner with a client. You cannot take your laptop with you to the restaurant. What should you do with the device? (Choose the best answer.)

a. Lock the laptop in your car trunk.

b. Store the laptop out of sight in a dresser drawer.

c. Secure the laptop to a piece of furniture with a laptop security cable.

d. Check the laptop at the front desk.

5. The process of eliminating a risk by choosing not to engage in an action or activity describes which of the following?

a. Mitigation

b. Residual risk

c. Avoidance

d. Acceptance

6. You have just been promoted to Chief Security Officer for your auto parts manufacturing business, and you are trying to identify technologies that will help ensure the confidentiality of your proprietary manufacturing techniques. Which of the following are technologies you could use to help with this endeavor? (Choose all that apply.)

a. Strong encryption

b. Security guards

c. Laptop safes

d. Strong authentication

7. The acronym CIA stands for which of the following?

a. Confidentiality, identity, access control

b. Confidentiality, integrity, access control

c. Confidentiality, integrity, availability

d. Control, identity, access control

8. You have been placed in charge of the corporate security department, and your boss has asked you to help her understand what is meant by core security principles. Which of these explanations should you give to your boss?

a. Core security principles refer to the internal security perimeter when setting up a layered physical security environment.

b. Core security principles refer to the principles of confidentiality, availability, and integrity.

c. Core security principles refer to leveraging security best practices.

d. Core security principles refer to the four methods of addressing risk.

9. As the Chief Security Officer for a small medical records processing company, you have just finished setting up the physical security for your new office. In particular, you have made sure that the parking lot is illuminated, that you have guards both at the door and performing periodic patrols, and that you have badge readers throughout the building at key locations. You also have put biometric access technology on the data center door. In

addition, you have cameras in the parking lot, at building entrances, and at the data center entrances. This type of implementation is known as: (Choose the best answer.)

a. Access control

b. Core security principles

c. Security best practices

d. Defense in depth

10. What do you call the process of disabling unneeded services and ports to make a system more secure?

a. Reducing the surface attack area

b. Mitigating a Trojan horse

c. Security avoidance

d. Defense in depth

Fill in the Blank

1. _____ is the characteristic of a resource that ensures that access is restricted to only permitted users, applications, or computer systems.

2. If you are deploying technologies to restrict access to a resource, you are practicing the security principle known as _____.

3. Deploying multiple layers of security technology is called _____.

4. An action or occurrence that could result in the breach, outage, or corruption of a system by exploiting known or unknown vulnerabilities is a(n) _____.

5. You have just taken a new job as the Risk Manager for a medium-sized pharmaceutical company, and your first assignment is to perform a formal risk assessment. You will most likely record the results of your risk assessment in a(n) _____.

6. A secretary at your office just got off the phone with someone who said he was calling from the corporate IT department. The caller had a number of questions about the secretary's computer setup, and he asked for her user ID and password. In this situation, the secretary was most likely a victim of _____.

7. The consistency, accuracy, and validity of data or information is called _____.

8. You are traveling for work and decide to use a computer in the hotel business center to check your email and pay several bills. When you sit down at the computer, you notice there is an extra connector between the keyboard and the computer. You have most likely encountered a(n) _____.

9. You are the Risk Manager for a regional bank, and you have just deployed a new badge reader system to address an access control risk. Although your solution has mitigated the risk, there is still a small remaining risk associated with access control. This risk is known as the _____.

10. The larger the _____ of a particular environment, the greater the risk of a successful attack.

Competency Assessment

Scenario 1-1: Designing a Physical Security Solution

You are the Security Manager for a medium-sized bank. You have been asked to design a security solution to keep intruders out of the bank after hours. The three areas of the bank you need to secure are the parking lot, the building perimeter, and the vault. List what technologies you would use in each of these areas.

Scenario 1-2: Securing a Mobile Device

You are the IT Manager for a 5,000-employee legal services company. You are in the process of rolling out new mobile devices to your sales department. What processes and technologies will you use to keep these systems physically secure?

Proficiency Assessment

Scenario 1-3: Looking at Confidentiality, Integrity, and Availability

Within your organization, you have a server called Server1 that is running Windows Server 2008 R2. On Server1, you create and share a folder called Data on the C drive. Within the Data folder, you create a folder for each user within your organization. You then place each person's electronic paycheck in his or her folder. Later, you find out that John was able to go in and change some of the electronic paychecks and delete others. Explain which of the CIA components was not followed in this scenario.

Scenario 1-4: Examining Social Engineering

You work for the Contoso Corporation. Your manager wants you to put together a training class about end-user security. To begin, use the Internet to research three cases or instances in which individuals used social engineering to break into a system, and list how they attempted to get access.

Workplace Ready

Understanding the Basics

Understanding security concepts is only the first step in learning about security. As a network administrator or security officer, you will be amazed by how much considering these basics will help you plan, implement, and update your organization’s overall security program.