Always remember that stealing a laptop with an unencrypted disk drive is faster than extracting the data from the device. **Physical security**, which is the collection of safeguards that limit physical access to assets, is just as important to overall information security as any technical control. The assets the security professional is charged with protecting are not just sitting “in an open field” someplace. Each asset has facilities and other physical barriers surrounding it.

Portable storage devices with sensitive data represent a real risk for the organization if they are lost, stolen, or misplaced. According to an article from Digicert.com, 45% of all health care data breaches are a direct result of stolen laptops. Encryption can be used on a file, a folder, an entire hard disk, or even a device’s available memory to provide a strong level of protection. Applying encryption to an entire disk is known as **full disk encryption** or **full volume encryption**. Full drive encryption, which is a technique that can be implemented in hardware or software, encrypts all the data on a selected volume or disk as selected by the owners of the system.

Software programs such as **Pretty Good Privacy (PGP)**, **TrueCrypt**, and **BitLocker**, can be used to lock files and folders. Microsoft offers data encryption programs, such as BitLocker and Encrypting File System (EFS), as part of the operating system in certain versions of Windows.

Hard drives should be **sanitized** when talking about disposing of media. Sanitization is the process of clearing all identified content so that no data remnants can be recovered. When sanitization is performed, none of the original information is easily recovered. Some of the methods used for sanitization are as follows:

* **drive wiping** – overwriting all information on the drive. As an example, NIST SP 800-88, “Guidelines for Media Sanitation”, provides details for multiple acceptable options for sanitizing different types of media.
* **Zeroization** – a process usually associated with cryptographic processes. The term was originally used with mechanical cryptographic devices. These devices would be reset to 0 to prevent anyone from recovering the key. In the electronic realm, zeroization involves overwriting the data with zeros. Zeroization is defined as a standard in ANSI X9.17.
* **Degaussing** – permanently destroys the contents of the hard drive or magnetic media. Degaussing works by means of a powerful magnet that uses its field strength to penetrate the media and reverse the polarity of the magnetic particles on the tape or hard disk platters.

Some software utilities that provide multiple levels of wiping include:

* **Active KillDisk**
* **Eraser**
* **Shred-it**
* **Disk Wipe**
* **Darik’s Boot and Nuke**

**VoIP** allows the placing of telephone calls over computer networks and the internet. VoIP has the capability to transmit voice signals as data packets over the network in real time and provide the same level of service as you would expect with traditional phone service. Techniques such as packet sniffing and capture can easily capture phone calls transmitted over the network; in fact, because of the sheer volume of calls that may be placed at any one time, a single attack can intercept and affect numerous calls.

Many attacks depend on **physical access**. For example, protected information can be extracted from a computer by simply booting the computer from a DVD or USB thumb drive. To do that, you need physical access to the computer. Simply having a few minutes of physical access can allow many attacks that may be very difficult to prevent or detect. To avoid these types of attacks, it is important to protect the physical access to your computers and devices as well as remote access to them.

Common controls placed at the perimeter of a facility can include many types of barriers that will physically and psychologically deter intruders:

* **Fences**
* **Perimeter intrusion detection and assessment systems (PIDASs)**
* **Gates**
* **Bollards**

**Fences** are one of the physical boundaries that provide the most visible and imposing deterrent. Depending on an organization’s needs, the purpose of erecting a fence may vary from stopping casual intruders to providing a formidable barrier to entry. Fences work well at preventing unauthorized individuals from gaining access to specific areas, but they also force individuals who have or want access to move to specific chokepoints to enter the facility.

In situations where a single fence fails to provide sufficient security, it is possible to layer other protective systems. For example, a **perimeter intrusion and detection assessment system (PIDAS)** can be used. This special fencing system works as an intrusion detection system (IDS) in that it has sensors that can detect intruders. Although these systems are expensive, they offer an enhanced level of protection over standard fences. In addition to cost, the downside of these systems is that it is possible that they may produce false positives from environmental factors, such as stray wildlife, high winds, or other natural events.

A **gate** is a chokepoint, or a point where all traffic must enter or exit the facility. All gates are not created equal, however, and if you select the incorrect one, you won’t get proper security. In fact, choosing the wrong gate can even detract from an otherwise effective security measure. A correctly chosen gate provides an effective deterrent and a barrier that will slow down an intruder, whereas an incorrectly chosen gate may not deter anyone but the casual intruder. **UL (Underwriters Laboratories)** Standard number 325 describes gate requirements. Gates are divided into 4 classifications:

* **residential, or Class 1** – these gates are ornamental in design and offer little protection from intrusion
* **commercial, or Class 2** – These gates are of somewhat heavier construction and fall in the range of 3 to 4 feet in height
* **industrial, or Class 3** – These gates are in the range of 6 to 7 feet in height and are of heavier construction, including chain-link construction
* **restricted access, or Class 4** – These gates must meet or exceed a height of 8 feet and are of heavier construction – iron bars, concrete, or similar materials. Gates in this category can include enhanced protective measures, including barbed wire.

**Bollards** are devices that can take many forms, but the goal is the same: to prevent entry into designated areas by vehicles. Bollards can come in many shapes, sizes, and types. Some are permanent, whereas others pop up as needed to block a speeding car from ramming a building, or ram-raiding. **Ram-raiding** is a type of smash-and-grab physical attack in which a heavy vehicle is driven through the windows or doors of a closed shop, usually one selling electronics or jewelry, to quickly rob it.

The weakest point of a structure is generally the first to be attacked. This means doors, windows, roof access, fire escapes, delivery access, and even chimneys are targets for attackers. You need strong facility controls and must provide only the minimum amount of access required and require and restrict unauthorized individuals from secure areas. Some ways to achieve these goals are:

* **doors**, **mantraps**, and **turnstiles**
* **walls**, **ceilings**, and **floors**
* **windows**
* **guards** and **dogs**
* **construction**

A solid-core door should always be used for the protection of a server room or other critical assets. Doors should also have a fire rating assigned to them, which is another item to consider before installing. Doors come in many configurations, including:

* **industrial doors**
* **vehicle-access doors**
* **bulletproof doors**
* **vault doors**

A **mantrap** is a structure that replaces a normal single door with a phone booth-sized space with a door on each side. When an individual enters the mantrap, there is enough space for only one person at a time, and only one door can be opened at a time. Although mantraps are designed to regulate the flow of traffic in and out of an area, they specifically stop piggybacking, which is the practice of one individual actually opening the door to let several enter. Another type of physical control device in common usage is the **turnstile**, which is commonly used at sporting events, subways, and amusement parks. Turnstiles can be used to slow the flow of traffic into areas or even ensure that individuals are properly screened and authenticated prior to entering an area.

Consider one of the more common mistakes that can be a detriment to security: **false walls**. They are walls that run from the floor up to the ceiling, but the ceiling isn’t real; it’s only a drop ceiling that has a good amount of space between it and the roof. If asked to perform a physical security assessment of a data center or other type of high-value physical asset, check to see that the wall runs past the drop ceiling. Also, tap on the wall gently to see whether it is hollow or of a solid construction.

For ceilings, the weight-bearing load and fire ratings must be considered. For drop ceilings, the walls should extend above the ceiling, especially in sensitive areas. Any ceiling-mounted air ducts should be small enough to prevent an intruder from crawling through them. The slab of the facility needs to have the proper weight load, fire rating, and drains. When dealing with raised floors, you will want to make sure the flooring is grounded and nonconducting. In areas with raised floors, the walls should extend below the false floor.

**Window** types include the following:

* **standard** – the lowest level of protection. They’re cheap and easily shattered and destroyed.
* **Polycarbonate acrylic** – much stronger than standard glass, this type of plastic offers superior protection.
* **Wire reinforced** – adds shatterproof protection and makes it harder for an intruder to break and access.
* **Laminated** – similar to what is used in an automobile. By adding a laminate between layers of glass, the strength of the glass is increased, and shatter potential is decreased.
* **Solar film** – provides a moderate level of security and decreases shatter potential.
* **Security film** – used to increase the strength of the glass in case of breakage or explosion.

Although computerized systems can provide vital security on the physical side, such systems have not reached the level where the human element can be replaced. **Guards** add discernment to onsite security. But guards are another example of where “you don’t get something for nothing.” Guards need to be screened before hiring, criminal background checks need to be performed, and sometimes security clearances must be obtained. Guards cost money. However, if a company does not have the money for a guard, there are other options. **Dogs** have been used for centuries for perimeter security. Although dogs are loyal, obedient, and steadfast, they are not perfect and might possibly bite or harm the wrong person because they do not have the level of discernment that human beings possess. Because of these factors, dogs are usually restricted to exterior premise control and should be used with caution.

**Construction** – The security professional is expected in most cases to provide input on the design or construction of a new facility or the functionality of a preexisting facility that the company is considering. When this situation arises, consider the following factors:

* what are the unique physical security concerns of the organization’s operations?
* Do redundancy measures exist (such as backup power or coverage by multiple telecom providers)?
* Is the location particularly vulnerable to vandalism?
* Are there any specific natural/environmental concerns for the specific region in which construction is being considered?
* Is the proposed construction close to military bases, train tracks, hazardous chemical production areas, or other hazards?
* Is the construction planned in high-crime neighborhoods?
* How close is the proposed construction to emergency services, such as the hospital, fire department, and police station?

**Any security plan must address the protection and security of personnel first and foremost**. The security of nonpersonnel assets is secondary. There is a wide assortment of technologies specifically designed to protect not only people but also the organization itself, including the following:

* lighting
* alarms and intrusion detection
* CCTV/remote monitoring

**Lighting** is perhaps one of the lowest-cost security controls that can be implemented by an organization. Lighting can provide increased security and a welcome sense of well-being to locations such as parking garages and building perimeters. When properly placed, lighting can eliminate shadows and reduce the areas that cameras or guards can’t monitor as well as reduce the places in which an intruder can hide. Some more common types of lights follow:

* **continuous** – fixed lights arranged to flood an area with overlapping cones of light (most common)
* **standby** – randomly turned on to create an impression of activity
* **movable** – manually operated movable searchlights; used as needed to augment continuous or standby lighting
* **emergency** – can duplicate any or all of the previous lights; depends on an alternative power source

Too much lighting can lead to a false sense of security because a company may feel that because all areas are lit, intrusion is unlikely. When placing lighting, avoid any placement that directs the lighting toward the facility and instead direct the lights toward fences, gates, or other areas of concern, such as access points.

Alarms and **physical intrusion detection** systems can also increase physical security. Both of these controls are referred to as detective controls. Detective controls only detect an event, as opposed to preventing it. Alarms typically are used to provide an alert mechanism if a potential intrusion, fire, or dangerous carbon monoxide level has been detected. One common problem with monitored alarm systems is the number of false alarms. This problem is such an issue for first responders that many services levy fines for excessive false alarms.

Additional options that can enhance physical intrusion detection include motion, audio, infrared wave pattern, and capacitance detection systems. Of these systems, infrared and motion detection tend to be the most common, but like any system, they have both pros and cons.

Another class of controls that can protect personnel and potentially deter crime is **closed-circuit TV (CCTV)** and other **remote monitoring** technologies. CCTV and remote monitoring usually work in conjunction with guards or other monitoring mechanisms to extend their capacity. They provide the ability to see what’s going on in a location in which a guard is not currently present. When dealing with surveillance devices, it is important to understand factors such as focal length, lens types, depth of field, and illumination requirements. The issue of focal length defines the camera’s effectiveness in viewing objects from a horizontal and vertical view. Short focal lengths provide wider-angle views, whereas longer focal lengths provide narrower views. Many of today’s CCTV systems depend on digital cameras connected to the organization’s network via wired or wireless connections. This type of CCTV monitoring system combines many aspects of physical and technical security.

A **physical access control** is any mechanism by which an individual can be granted or denied physical access. One of the oldest forms of access control is the mechanical lock.

**Locks**, which come in many types, sizes, and shapes, are an effective means of physical access control. Locks are by far the most widely implemented security control largely because of the wide range of options available as well as the low cost of the devices. Lock types include the following:

* **mechanical** – warded and pin and tumbler
* **cipher** – smart and programmable

Warded locks are the simplest form of mechanical lock. The design of mechanical locks uses a series of wards that a key must match in order to open the lock. Although it is the cheapest type of mechanical lock, it is also the easiest to pick. Pin and Tumbler locks are considered more advanced. These locks contain more parts and are harder to pick than warded locks. More advanced and technically complex than warded or pin and tumbler locks are cipher locks, which have a keypad of fixed or random numbers that requires a specific combination to open the lock. The grade of lock specifies its level of construction. The 3 basic grades are:

* **grade 1** – commercial locks with the highest security
* **grade 2** – light-duty commercial locks or heavy-duty residential locks
* **grade 3** – consumer locks with the weakest designated

The basic components used to pick locks follow:

* **tension wrenches** – like small, angled flathead screwdrivers. They come in various thicknesses and sizes.
* **Picks** – just as the name implies, similar to dentist picks: small, angled, and pointed.

**Tokens** are available in many types and can range from basic ID cards to more intelligent forms of authentication systems. Tokens used for authentication can make an access decision electronically and come in several different configurations, including:

* **active electronic** – the access card has the ability to transmit electronic data.
* **Electronic circuit** – the access card has an electronic circuit embedded.
* **Magnetic stripe** – the access card has a stripe of magnetic material.
* **Contactless cards (proximity cards)** – the access card communicates with the card reader electronically without requiring physical contact with the reader. Contactless cards do not require the card to be inserted or slid through a reader. These devices function by detecting the proximity of the card to the sensor. An example is the **RFID** chip.

Another form of authentication control is **biometrics**. Biometric authentication is based on behavioral or physiological characteristic that is unique to an individual. Biometric authentication systems have gained market share because they are seen as a good replacement for password-based authentication systems. The accuracy of a biometric device is measured by the percentage of type 1 and type 2 errors it produces. Type 1 errors, or false rejections, are reflected by what is known as the **false rejection rate (FRR)**. This is a measurement of the percentage of individuals who should have been granted but were not allowed access. A type 2 error, or false acceptance, is reflected by the **false acceptance rate (FAR)**, which is a measurement of the percentage of individuals who have gained access but should not have been granted access. Some biometric systems include:

* **finger scan systems** – widely used, popular, installed in many new laptops and mobile devices
* **hand geometry systems** – accepted by most users; function by measuring the unique geometry of a user’s fingers and hand to determine an identity
* **palm scan systems** – much like the hand geometry systems except they measure the creases and ridges of a user’s palm for identification
* **retina pattern systems** – very accurate; examine the user’s retina pattern
* **iris recognition** – another eye recognition system that is also very accurate; matches the person’s blood vessels on the back of the eye
* **voice recognition** – determines identity by using voice analysis
* **keyboard dynamics** – analyze the user’s speed and pattern of typing

Some common threats include the following:

* natural, human, and technical threats
* physical keystroke loggers and sniffers
* wireless interception and rogue access points

Human threats include the following:

* **theft** – theft of company assets can range from mildly annoying to extremely damaging.
* **Vandalism** – a teenager just having some malicious fun by breaking windows and a hacker who decides to change your company’s web page are both destroying company property.
* **Destruction** – this threat can come from insiders or outsiders. Destruction of physical assets can cost organizations money that was budgeted to be spent on other items.
* **Terrorism** – this form of threat is posed by individuals or groups that wish to prove a point or draw attention to a cause.
* **Accidental** – accidents are bound to happen sooner or later, and their effects can be varied depending on the situation. Damage could range from lost data to attackers having access they shouldn’t have.

Hardware **keystroke loggers** are physical devices used to record everything a person types on the keyboard. These devices are usually installed while the user is away from the desk. Keystroke loggers can be used for legal or illegal purposes:

* monitoring employee productivity and computer activity
* law enforcement
* illegal spying

They can be:

* attached to the keyboard cable, as inline devices
* installed inside standard keyboards
* installed inside replacement keyboards
* installed as software on a system along with other software

**Sniffing** is the basic technique used for a large number of network-based attacks. If attackers can gain access to the network via a physical network connection, they can begin to capture traffic. Sniffing can be passive or active. Passive sniffing relies on a feature of network cards called “promiscuous mode.” When placed in promiscuous mode, a network card passes all packets on the operating system rather than just those unicast or broadcast to the host. Active sniffing, on the other hand, relies on injecting packets into the network, causing traffic that should not be sent to your system to be sent to your system.

**Bluetooth** is a short-range communication technology that has been shown to be vulnerable to attack. One such attack is Bluejacking, which allows an individual to send unsolicited messages over Bluetooth to other Bluetooth devices. WLANs are vulnerable to attacks as well. These attacks can be categorized into 4 basic categories: eavesdropping, open authentication, rogue access points, and denial of service.

The concept of **defense in depth** originated from the military and was seen as a way to delay rather than prevent an attack. As an information security tactic, it is based on the concept of layering more than one control to protect assets. These controls can be physical, administrative, or technical in design.

For the physical facility, a security professional should strive for a minimum of 3 layers of physical defense. The first line of defense is the building perimeter. Barriers placed here should delay and deter attacks. Items at this layer include fences, gates, and bollards. These defenses should not reduce visibility of CCTV and/or guards. Items such as shrubs should be 18-24 inches away from all entry points, and hedges should be cut 6 inches below the level of all windows.

The 2nd layer of defense is the building exterior: roof, walls, floor, doors, and ceiling. Windows are a weak point here. Any opening 18 feet or less above the ground should be considered a potential easy access and should be secured if greater than 96 square inches.

The 3rd layer of physical defense is the interior controls: locks, safes, containers, cabinets, interior lighting. It can even include policies and procedures that cover what controls are placed on computers, laptops, equipment, and storage media. This third layer of defense is important when you consider items such as the data center or any servers kept onsite. A well-placed data center should not be above the second floor of a facility because a fire might make it inaccessible. Likewise, you wouldn’t want the data center located in the basement, because it might be subject to flooding.

1. Physical security is less important than logical security.

* True
* False

2. \_\_\_\_\_\_\_ is a common physical control that can be used as both a detective and a reactive tool.

* A fence
* an alarm
* CCTV
* a lock

3. For a fence to deter a determined intruder, it should be at least \_\_\_\_\_\_ feet tall.

* 4
* 5
* 8
* 10

4. A(n) \_\_\_\_\_\_\_\_ is used to prevent cars from ramming a building.

* Bollards

5. Although both guards and dogs are good for physical security, which of the following more commonly applies to dogs?

* Liability
* discernment
* dual role
* multifunction

6. What grade of lock would be appropriate to protect a critical business asset?

* Grade 4
* grade 2
* grade 1
* grade 3

7. \_\_\_\_\_\_\_\_ defines the camera’s effectiveness in viewing objects from a horizontal and vertical view.

* Granularity
* ability to zoom
* field of view
* focal length

8. In the field of IT security, the concept of defense in depth is layering more than one control on another.

* True
* False

9. \_\_\_\_\_\_\_ is an intrusion detection system used excessively in conjunction with fences.

* Infrared wave patter
* motion detector
* RFID
* PIDAS

10. A type 2 error is also known as what?

* False rejection rate
* failure rate
* crossover error rate
* false acceptance rate

11. Which type of biometric system is frequently found on laptops?

* Retina
* fingerprint
* iris
* voice recognition

12. What do lock pick sets typically contain, at a minimum?

* Tension wrenches and drivers
* a pick
* a pick and a driver
* a pick and a tension wrenches

13. During an assessment, you discovered that the target company was using a fax machine. Which of the following is the least important?

* The phone number is publicly available
* the fax machine is in an open, unsecured area
* faxes frequently sit in the printer tray
* the fax machine uses a ribbon