Covers all Exam Objectives for CEHv6

Includes Real-World Scenarios, Hands-On Exercises, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards
- Entire Book in PDF

CEH™

Certified Ethical Hacker

STUDY GUIDE

Exam 312-50
Exam ECO-350

Kimberly Graves

SYBEX | SERIOUS SKILLS.

Table of Contents

Chapter

11

Physical Site Security

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Physical security breach incidents**
- ✓ **Understanding physical security**
- ✓ **What is the need for physical security?**
- ✓ **Who is accountable for physical security?**
- ✓ **Factors affecting physical security**

Physical security is arguably the most critical area of IT security for preventing the loss or theft of confidential and sensitive data. If an organization fails to enforce adequate physical security, all other technical security measures such as firewalls and intrusion detection systems (IDSs) can be bypassed. There is a saying: "Once you're inside, you own the network." By physically securing your network and your organization, you prevent somebody from stealing equipment such as laptops or tape drives, placing hardware keyloggers on systems, and planting rogue access points on the network. Physical security relies heavily on individuals to enforce it and therefore is susceptible to social-engineering attacks, such as following an employee into the building without supplying the proper key or credentials (thus bypassing the physical security challenge).

This chapter will explore the need for physical security and define who is responsible for planning and enforcing it.

Components of Physical Security

Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

Physical security is often overlooked (and its importance underestimated) in favor of more technical and dramatic issues such as hacking, viruses, Trojans, and spyware. However, breaches of physical security can be carried out with little or no technical knowledge on the part of an attacker. Moreover, accidents and natural disasters are a part of everyday life, and in the long term, are inevitable.

There are three main components to physical security:

- Obstacles can be placed in the way of potential attackers and sites can be hardened against accidents and environmental disasters. Such measures can include multiple locks, fencing, walls, fireproof safes, and water sprinklers.
- Surveillance and notification systems, such as lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras, can be put in place.
- Methods can be implemented to apprehend attackers (preferably before any damage has been done) and to recover quickly from accidents, fires, or natural disasters.

It seems as though every day, a news article describes another prominent government agency or major corporation that has compromised client information or confidential employee information. For example, a laptop may be stolen in a home-invasion robbery or from a hotel room while an employee is traveling. This confidential or sensitive information can be dangerous in the hands of a hacker.

In physical security, like all security, the best approach is a layered defense. You should never depend 100 percent on a single control to protect your critical assets. Here are two examples of where a layered approach to physical security is better than a single physical security mechanism.

The first example is when a guard is the only defense mechanism in place. If he falls asleep or takes an unscheduled break, then an intruder has the opportunity to walk right into your data center without being detected. A better security measure would be to have an individual be required to possess a unique ID badge to enter the front door. Next, she is challenged by a guard, recorded on a camera, and then needs to have a separate unique key to enter the data center. In this example, there are four layers of defense to protect your assets.

In the second security example, an employee can't afford a laptop, so he decides to take his company computer home to play his favorite video game. He gets distracted on the train or bus on the way home and forgets his bag containing the laptop. The laptop does not have any security controls in place and contains sensitive data. If best practices were followed in this scenario, multiple layers would exist to prevent and discourage this individual from removing the laptop from the controlled environment. An acceptable use policy should be in place to stress the importance and ramifications of removing corporate property and sensitive data from the premises. The laptop should have multi-factor authentication and disk encryption enabled, so that in the event that it is lost or stolen, the data that existed on it is useless to others. If the environment were particularly sensitive, tracking devices could be placed in all mobile devices, and in the event that they travel an unacceptable distance from the office, an alarm is activated to notify security personnel.

It is critical to have multiple lines of defense, as the more layers of defense you have in place, the less vulnerable you are to a threat. Also it is important to remember that you can have many layers of logical security controls protecting an asset and they can generally be circumvented quickly and easily if physical access is gained.

Equipment theft is one of the most common physical security attacks. Most people don't expect their computer to be stolen and are naive about locking down host systems; instead, they rely on standard network security mechanisms.

Many insider attacks are the result of physical security breaches. Once a hacker has gained physical access to a server, a single client system, or a network port, the results can be disastrous. In addition, such breaches are difficult to identify, track, or locate. Some of the common security breaches caused by insufficient physical security are as follows:

- Installation of malware such as keyloggers, viruses, Trojans, backdoors, or rootkits
- Identification and capture of validation or authentication credentials such as passwords or certificates
- Physical connection to the wired network to sniff confidential data such as passwords and credit card numbers

- Access to systems to collect data that can be used to crack passwords stored locally on the system
- Opportunity to plant rogue access points to create an open wireless network with access to the wired network
- Theft of paper or electronic documents
- Theft of sensitive fax information
- Dumpster diving attack (emphasizing the need to shred important documents)

Indications of a physical security breach may include, but are not limited to

- Unauthorized or unexplained door alarms
- Unauthorized personnel recorded on a security camera
- Damage to door lock or outside barrier fence
- Evidence of vehicles or persons outside and inside the perimeter fence
- Loss of communications that cannot be explained
- Missing or unaccounted for equipment

Understanding Physical Security

Generally security measures can be categorized in the following three ways:

Physical Physical measures to prevent access to systems include security guards, lighting, fences, locks, and alarms. Facility access points should be limited, and they should be monitored/protected by closed-circuit television (CCTV) cameras and alarms. The entrance to the facility should be restricted to authorized people. Access to laptop systems and removable media such as removable drives, backup tapes, and disks should be restricted and protected. Computer screens should be positioned such that they can't be seen by passers-by, and a policy should be implemented and enforced that requires users to lock their systems when they leave the computer for any reason. Computer systems with highly sensitive data should be protected in an enclosed and locked area such as a credential-access room with a rack-mount case and lock.

Technical Technical security measures such as firewalls, IDS, spyware content filtering, and virus and Trojan scanning should be implemented on all remote client systems, networks, and servers. Technical security measures such as access control are implemented through the use of authentication, passwords, and file and folder permissions. Other technical controls can be implemented through computer software such as virus scanning and host firewalls. Essentially a technical control is any security mechanism implemented through computer hardware or software.

Operational Operational security is addressed through administrative controls such as acceptable use policies, hiring policies, and security policies. Operational security measures

to analyze threats and perform risk assessments should be a documented process in the organization's security policy.

Technical and operational security measures are dealt with in other chapters of this book. Technical countermeasures are listed in every chapter of this book (except the first and last chapters).

You need physical security measures for the same reason you need other types of security (such as technical or operational): to prevent hackers from gaining access to your network and your information. A hacker can easily get such access through weaknesses in physical security measures. In addition, data can be lost or damaged by natural causes, so risk managers must add natural disasters to the equation when planning appropriate security. Physical security measures are designed to prevent the following:

- Unauthorized access to a computer system
- Stealing of data from systems
- Corruption of data stored on a system
- Loss of data or damage to systems caused by natural causes

Real World Scenario

Data Stolen from VA Laptop

In 2006, a laptop computer was stolen from the home of a Department of Veterans Affairs data analyst who (against department policy) took the computer home. The laptop contained data on about 26.5 million U.S. military veterans.

It is believed that this was a random burglary and the person who stole the laptop did not know the data was on the computer. The thieves took both his laptop and the external hard drive containing names, birth dates, and Social Security numbers of every veteran who had been discharged after 1975.

The VA commented that the employee "took home a considerable amount of electronic data from the VA which he was not authorized to do. It was in violation of our rules and regulations and policies." This security breach is an example of how your most personal data can easily get into the hands of identity thieves.

Several veterans groups took legal action against the VA after the breach was discovered. Now, three years later, the parties have come to an agreement. Veterans who can show proof of actual harm, such as emotional distress leading to physical symptoms, or expenses for credit monitoring, will be eligible to receive payments up to $1,500. This settlement totals $20 million in costs to the VA. This is just one example of how important physical site security and enforcing policies is to maintain security for personal data. Organizations found liable for not protecting the data to which they have been entrusted may face heavy fines.

The following people in an organization should be accountable for physical security:

- The organization's physical security officer
- Information system professionals
- Chief information officer
- Employees

Essentially, everyone in an organization is responsible for enforcing physical security policies. It's the physical security officer's responsibility to set the physical security standard and implement physical security measures.

Organizations have a responsibility to train all employees in security awareness training. The best countermeasure to prevent physical security attacks is to train employees to be aware of breaches to physical security.

Physical security is affected by factors outside the physical security controls. Factors that can affect an organization's physical security include the following:

- Vandalism
- Theft
- Natural causes, such as earthquake, fire, or flood

Security professionals need to be aware of these risk factors and plan accordingly. Many organizations create a business continuity plan (BCP) or disaster recovery plan (DRP) to prepare for these possibilities.

Physical Site Security Countermeasures

There are some simple ways to improve physical security in your organization. Many times improving security involves enforcing the guidelines that are already in place. People tend to get loose in their enforcement of policies and procedures after a period of time. To maintain a high level of security, everyone in the organization must be vigilant in protecting the data assents of the organization.

The following countermeasures should be implemented to ensure strong physical site security:

Lock the server room. Before you lock down the servers using technical mechanisms and before you even turn them on for the first time, you should ensure that there are good locks on the server room door. Of course, the best lock in the world does no good if it isn't used, so you also need policies requiring that those doors be locked any time the room is unoccupied. The policies should set out who has the key or keycode to get in. The server room is the heart of your physical network, and someone with physical access to the servers, switches, routers, cables, and other devices in that room can do enormous damage.

Set up and monitor video surveillance. Locking the door to the server room is a good first step, but someone could break in, or someone who has authorized access could misuse that authority. You need a way to know who goes in and out and when. A log book for signing in and out is the most elemental way to accomplish this, but that approach has a lot of drawbacks. A person with malicious intent is likely to just bypass it. A better solution than the log book is an authentication system incorporated into the locking devices, so that a smart card, token, or biometric scan is required to unlock the doors and a record is made of the identity of each person who enters. A video surveillance camera, placed in a location that makes it difficult to tamper with or disable but gives a good view of persons entering and leaving, should supplement the log book or electronic access system. Surveillance cameras can monitor continuously, or they can use motion detection technology to record only when someone is moving about. They can even be set up to send email or cell phone notification if motion is detected when it shouldn't be, such as after hours.

Make sure the most vulnerable devices are in a locked room. It's not just the servers that you have to physically secure. Other networking equipment also needs to be secured. A hacker can plug a laptop into a hub and use sniffer software to capture data traveling across the network. Make sure that as many of your network devices as possible are in that locked room. Wiring closets and phone rooms are easy targets if not secured.

Secure the workstations. Hackers can use any unsecured computer that's connected to the network to access or delete information that's important to your business. Workstations at unoccupied desks or in empty offices—such as those used by employees who are on vacation or who have left the company and not yet been replaced—or at locations easily accessible to outsiders—such as the front receptionist's desk—are particularly vulnerable. Disconnect and/or remove computers that aren't being used and/or lock the doors of empty offices, including those that are temporarily empty while an employee is at lunch or out sick. For computers that must remain in open areas, sometimes out of view of employees, enable smart card or biometric readers so that it's more difficult for unauthorized persons to log on.

Keep intruders from opening the computer. Both servers and workstations should be protected from thieves who can open the case and grab the hard drive. It's much easier to make off with a hard disk in your pocket than to carry a full tower off the premises. Many computers come with case locks to prevent opening the case without a key.

Protect the portable devices. Laptops and handheld computers pose special physical security risks. A thief can easily steal the entire computer, including any data stored on its disk as well as network logon passwords that may be saved. If employees use laptops at their desks, they should take them along when they leave or secure them to a permanent fixture with a cable lock. Handhelds can be locked in a drawer or safe when the employee leaves the area. Motion-sensing alarms are also available to alert you if your portable is moved. For portables that contain sensitive information, full disk encryption, biometric readers, and software that "phones home" if the stolen laptop connects to the Internet can supplement physical precautions.

Many smart phones have the ability to do a remote wipe if a device is lost or stolen.

Pack up the backups. Backing up important data is an essential element in disaster recovery, but don't forget that the information on those backup tapes, disks, or discs can be stolen and used by someone outside the company. Many IT administrators keep the backups next to the server in the server room. They should be locked in a drawer or safe at the very least. Ideally, a set of backups should be kept off site, and you must take care to ensure that they are secured in that offsite location. Don't overlook the fact that some workers may back up their work on floppy disks, USB keys, or external hard disks. If this practice is allowed or encouraged, be sure to have policies requiring that the backups be locked up at all times.

Disable removable media drives. To prevent employees from copying company information to removable media, you can disable or remove floppy drives, USB ports, and other means of connecting external drives. Simply disconnecting the cables may not deter technically savvy workers. Some organizations go so far as to fill ports with glue or other substances to permanently prevent their use, although there are software mechanisms that disallow that and allow for an administrator to reenable the drive.

Protect your printers. You might not think about printers posing a security risk, but many of today's printers store document contents in their own onboard memories. If a hacker steals the printer and accesses that memory, he or she may be able to make copies of recently printed documents. Printers, like servers and workstations that store important information, should be located in secure locations and bolted down so nobody can walk off with them. Also think about the physical security of documents that workers print out. It's best to implement a policy of immediately shredding any unwanted printed documents, even those that don't contain confidential information. This establishes a habit and frees the end user of the responsibility for determining whether a document should be shredded.

Enforce badges for all employees and contractors. Initiate a badge program that includes an employee picture, and color-code specific areas of access. Contractors and visitors should also have badges and be escorted, observed, and supervised for their entire visit. It should be standard policy for all employees to question anyone who doesn't have a visible ID badge.

Watch out for "tailgaters." These people wait for someone with access to enter a controlled area such as one with a locked door and then follow the authorized person through the door. Tailgaters enter without using their own key, card key, or lock combination. Smokers who stand outside the building seem to be especially susceptible to "tailgating"; after sharing some time and a smoke together, it is normal to hold the door open for other smokers when the smoke break is over.

Exercise 11.1 is viewing a video on lockpicking. It is useful to understand how to pick a lock in order to understand how an intruder can gain physical access.

EXERCISE 11.1

View a Video on Lockpicking

1. Open a web browser to `www.youtube.com`.
2. Search for "lock picking video" or "lock picking door".
3. Watch a video on lock picking.
4. Search for "How Lock Picking Works" on `www.howstuffworks.com`.
5. Follow the interactive tutorial on using the correct and incorrect keys in a lock.
6. Answer the following questions about lock picking based on the YouTube video and HowStuffWorks tutorial:
   - What is the purpose of a tension wrench?
   - How do you keep the tumblers from falling down when picking a lock?
   - What is raking?
   - What is the shear line?
   - What types of locks are the most difficult to pick?

Not all attacks on your organization's data come across the network, and not all attacks are technical in nature. It's imperative that companies remember that maintaining a strong network security program doesn't immunize them against the physical assault or theft of data and the resources that contain that data. Physical attacks can be from outside an organization, but they can also be insiders—disgruntled employees or contractors are commonly found to be the source of physical site attacks. See Exercise 11.2.

EXERCISE 11.2

Audit Your Organization's Physical Site Security

Review the following physical site security checklist to evaluate your organization's physical security.

Public Parking Areas

- If appropriate, are employee, tenant, and public parking areas clearly designated?
- Are nighttime lighting levels adequate? *Test: Can you comfortably read a newspaper under existing lighting conditions?*
- Are parking areas and entrances observable by as many people as possible?
- Are parking areas fully lit during all hours that people are on the property?

EXERCISE 11.2 *(continued)*

- If appropriate, have parking areas been properly posted to permit law enforcement personnel to take enforcement action when necessary? *Examples: restricted parking zones, handicapped parking.*

Restricted Access Areas

- Are barriers such as fences and locked gates installed to prevent unauthorized vehicle and pedestrian access to restricted areas?
- Are employees instructed to report unauthorized individuals in restricted areas and other suspicious persons and activities?
- Are restricted areas properly posted to keep out unauthorized individuals?
- Is outdoor signage prominently displayed near areas of restricted access?
- Is signage indicating the phone number for reporting suspicious activity in an easy-to-see location?

Storage Areas

- Are outside storage areas and yards fully enclosed?
- Are fences and walls in good repair?
- Are fences high enough?
- Are gates in good repair?
- Are storage areas and yards provided with adequate lighting during the hours of darkness?
- Are gates secured with high security padlocks or equivalent locking devices?
- Are padlocks locked in place when gates open?
- Are high value storage areas protected by an electronic security system?

Building Exterior

- Are public entrances clearly defined by walkways and signage?
- Are landscape features maintained to provide good visibility around buildings?
- Is vegetation trimmed to eliminate potential hiding places near doors, windows, walkways, and other vulnerable areas of the property?
- Do trees or other landscape features provide access to the roof or other upper levels of buildings?
- Are trees and vegetation kept trimmed to prevent them from interfering with lighting and visibility?

EXERCISE 11.2 *(continued)*

- Do dumpsters and trash enclosures create blind spots or hiding areas?
- Are perimeter fences designed to maintain visibility from the street?
- Are exterior private areas easily distinguishable from public areas?

Lighting

- Are building exteriors and other critical areas illuminated to recommended levels during hours of darkness?
- Are proper lighting levels maintained at all door and window openings and other vulnerable points during hours of darkness?
- Has a maintenance inspection schedule been established to ensure that lights are in good working order at all times?

Doors

- Are all exterior doors of a metal, metal and glass, or solid core wood design?
- Are all unused doors permanently sealed?
- Is exterior hardware removed from all doors that are not used to provide access from the outside?
- Are all doors designed so that the lock release cannot be reached by breaking out glazing or lightweight panels?
- Are sliding glass doors equipped with supplemental pin locks and anti-lift devices?
- Do exposed hinges have nonremovable pins?
- Is a good-quality deadbolt lock used whenever possible?
- Is the lock designed, or the doorframe constructed, so that the door cannot be forced open by spreading the frame?
- Are keys issued only to persons who actually need them?
- Is there a policy in place mandating that all doors that are not required to be unlocked during business hours be closed and secured when not in use?

Windows

- Are unused windows permanently sealed?
- Are window locks designed or located so they cannot be defeated by breaking the glass?
- Where appropriate, are landscaping features such as thorny shrubs or similar vegetation used to prevent access to vulnerable windows?

EXERCISE 11.2 *(continued)*

- Where necessary, are accessible windows adequately lit during hours of darkness?
- Are roof ladders and other roof access points either removed or secured against unauthorized use?
- Are roll-up and sliding doors properly mounted and secured with high-quality locking devices?
- Are utility rooms both inside and outside the building properly secured?

Public Access Areas

- Are security and/or reception areas positioned to view all public entrances?
- Are all public areas of the building clearly marked?
- Are the boundaries between public and nonpublic areas clearly defined?
- Have secure barriers been installed to prevent easy movement between public and nonpublic areas?
- Are all doors leading to private offices and other nonpublic areas secured by high-quality locking devices such as electronic or keypad style locks?
- Are security guards employed in areas where there is a strong likelihood of criminal activity or trespassing?
- Are interior public restrooms observable from nearby offices or reception areas?

Office Security

- Do you restrict office keys to those who actually need them?
- Do you keep complete, up-to-date records of the disposition of all office keys?
- Do you have adequate procedures for collecting keys from terminated employees?
- Do you secure all typewriters, calculators, computers, and similar items with some type of locking device?
- Do you prohibit duplication of office keys except for those that are specifically ordered by you in writing?
- Do you require that all office keys be marked "Do not duplicate" to prevent legitimate locksmiths from making copies without your knowledge?
- Have you established a policy that keys will not be left unguarded on desks or cabinets—and do you enforce the policy?

EXERCISE 11.2 *(continued)*

- Have you established a policy that facility keys and key rings will not be marked with information that identifies the facility to which they belong?
- Do you require that filing cabinet keys be removed from locks and placed in a secure location when not in use?
- Do you have a responsible person in charge of your key-control program?
- Do you shred sensitive documents before discarding them?
- Do you lock briefcases and bags containing important material in a safe place when not in use?
- Do you insist on proper identification from all vendors and repair persons who come into your facility?
- Do you clear desks of important papers every night?
- Do you frequently change the combination to your safe?
- Is computer access restricted to authorized personnel?
- Have you instituted an employee identification badge system?
- If you employ guards after hours, do you periodically make unannounced visits to ensure that they are doing their job properly?

Alarms

- Do your buildings have an alarm system?
- Is the alarm system certified by Underwriters Laboratory?
- Is the system tested daily?
- Does the system report to an alarm company central station or police facility?
- Does the system have an automatic backup power supply that activates during power failures?
- Is the system free from false alarms?
- Does the system employ anti-tamper technology?

What to Do After a Security Breach Occurs

Even if an organization applies physical site countermeasures, a security breach may still occur. If such a breach occurs, there are some recommended steps your organization should take to prevent it from occurring again:

- Establish a physical security incident response process, including identification of the threat, response, recovery, and post-incident review to manage a physical attack or security incident.
- Set policies, standards, and procedures to support the physical security incident response process.
- Identify the stakeholders—including the security incident response team, personnel within the organization, and external parties who are likely to be involved in managing and reviewing the information security incident.

Summary

Remember that network security starts at the physical level. All the firewalls in the world won't stop an intruder who is able to gain physical access to your network and computers, so lock up as well as lock down. Physical access to corporate data by an unauthorized person is an assault on your organization's security. Once someone gains physical access to your data—whether it's a stolen laptop or lost documents or media—you become vulnerable to further attacks, not to mention a lot of bad publicity. It is critical to implement physical site security measures to prevent attacks before they occur.

Exam Essentials

Understand the attacks that can be performed via physical access. Physical access gives a hacker the ability to perform password cracking, install rogue wireless access points, and steal equipment.

Know some factors that affect the enforcement of physical security. Vandalism, theft, and natural causes affect the enforcement of physical security.

Know who is accountable for physical security. The organization's security officer, information system professionals, chief information officer, and employees are all responsible for physical security.

Understand the need for physical security. Physical security is necessary to prevent unauthorized access to a building or computer system, theft of data, corruption of data stored on a system, and loss of data or damage to systems caused by natural causes.

Review Questions

1. Who is responsible for implementing physical security? (Choose all that apply.)
   - **A.** The owner of the building
   - **B.** Chief information officer
   - **C.** IT managers
   - **D.** Employees
2. Which of these factors impacts physical security?
   - **A.** Encryption in use on the network
   - **B.** Flood or fire
   - **C.** IDS implementation
   - **D.** Configuration of firewall
3. Which of the following is physical security designed to prevent? (Choose all that apply.)
   - **A.** Stealing confidential data
   - **B.** Hacking systems from the inside
   - **C.** Hacking systems from the Internet
   - **D.** Gaining physical access to unauthorized areas
4. Which of the following is often one of the most overlooked areas of security?
   - **A.** Operational
   - **B.** Technical
   - **C.** Internet
   - **D.** Physical
5. A hacker who plants a rogue wireless access point on a network in order to sniff the traffic on the wired network from outside the building is causing what type of security breach?
   - **A.** Physical
   - **B.** Technical
   - **C.** Operational
   - **D.** Remote access
6. Which area of security usually receives the least amount of attention during a penetration test?
   - **A.** Technical
   - **B.** Physical
   - **C.** Operational
   - **D.** Wireless

7. Which of the following attacks can be perpetrated by a hacker against an organization with weak physical security controls?
   - **A.** Denial of service
   - **B.** Radio frequency jamming
   - **C.** Hardware keylogger
   - **D.** Banner grabbing

8. Which type of access allows passwords stored on a local system to be cracked?
   - **A.** Physical
   - **B.** Technical
   - **C.** Remote
   - **D.** Dial-in

9. Which of the following is an example of a physical security breach?
   - **A.** Capturing a credit card number from a web server application
   - **B.** Hacking a SQL Server in order to locate a credit card number
   - **C.** Stealing a laptop to acquire credit card numbers
   - **D.** Sniffing a credit card number from packets sent on a wireless hotspot

10. What type of attack can be performed once a hacker has physical access?
    - **A.** Finding passwords by dumpster diving
    - **B.** Stealing equipment
    - **C.** Performing a DoS attack
    - **D.** Performing session hijacking

11. What is the most important task after a physical security breach has been detected?
    - **A.** Lock down all the doors out of the building.
    - **B.** Shut down the servers to prevent further hacking attempts.
    - **C.** Call the police to begin an investigation.
    - **D.** Gather information for analysis to prevent future breaches.

12. Which of the following is a recommended countermeasure to prevent an attack against physical security?
    - **A.** Lock the server room.
    - **B.** Disconnect the servers from the network at night.
    - **C.** Do not allow anyone in the server room.
    - **D.** Implement multiple ID checks to gain access to the server room.

13. What are some physical measures to prevent a server hard drive from being stolen? (Choose all that apply.)
    A. Lock the server room door.
    B. Lock the server case.
    C. Add a software firewall to the server.
    D. Enforce badges for all visitors.

14. What is the name for a person who follows an employee through a locked door without their own badge or key?
    A. Tailgater
    B. Follower
    C. Visitor
    D. Guest

15. Which of the following should be done after a physical site security breach is detected?
    A. Implement security awareness training.
    B. Establish a security response team.
    C. Identify the stakeholders.
    D. Perform penetration testing.

16. Which of the following should be physically secured? (Choose all that apply.)
    A. Network hubs/switches
    B. Removable media
    C. Confidential documents
    D. Backup tapes
    E. All of the above

17. Which of the following are physical ways to protect portable devices? (Choose all that apply.)
    A. Strong user passwords
    B. Cable locks to prevent theft
    C. Motion-sensing alarms
    D. Personal firewall software

18. Which of the following are physical security measures designed to prevent?
    A. Loss of data or damage to systems caused by natural causes
    B. Access to data by employees and contractors
    C. Physical access to a customer database
    D. Access to an employee database via the Internet

19. Which of the following could be caused by a lack of physical security?
    - **A.** Web server attack
    - **B.** SQL injection
    - **C.** Attack on a firewall
    - **D.** Implementation of a rogue wireless access point

20. Which of the following are indications of a physical site breach?
    - **A.** Unauthorized personnel recorded on a security camera
    - **B.** IDS log event recording an intruder accessing a secure database
    - **C.** An antivirus scanning program indicating a Trojan on a computer
    - **D.** An employee inappropriately accessing the payroll database

Answers to Review Questions

1. B, C, D. The chief information officer, along with all the employees, including IT managers, is responsible for implementing physical security.
2. B. A fire or flood can affect physical security; all the other options are technical security issues.
3. A, B, D. Physical security is designed to prevent someone from stealing confidential data, hacking systems from the inside, and gaining physical access to unauthorized areas. Technical security defends against hacking systems from the Internet.
4. D. Physical security is one of the most overlooked areas of security.
5. A. In order to place a wireless access point, a hacker needs to have physical access.
6. B. Physical security usually receives the least amount of testing during a penetration test.
7. C. A hardware keylogger can be installed to capture passwords or other confidential data once a hacker gains physical access to a client system.
8. A. Physical access allows a hacker to crack passwords on a local system.
9. C. Theft of equipment is an example of a physical security breach.
10. B. Stealing equipment requires physical access.
11. D. The most important task after a physical security breach has been detected is to gather information and analyze to prevent a future attack.
12. A. Locking the server room is a simple countermeasure to prevent a physical security breach.
13. A, B, D. Locking the server room and server cases and enforcing badges for all visitors are physical controls. A software firewall is a technical control.
14. A. A tailgater is the name for an intruder who follows an employee with legitimate access through a door.
15. C. After a physical site security breach, the stakeholders in the incident response process need to be identified. Implement security awareness training, establish a security response team, and perform penetration testing before another physical site security breach is detected.
16. E. Network hubs and switches, removable media, confidential documents, and all backup media tapes should be physically secured and then destroyed when they are no longer needed.

17. B, C. Cable locks and motion-sensing alarms are physical countermeasures to prevent theft of portable devices.

18. A. Physical security measures are designed to prevent loss of data or damage to systems caused by natural causes.

19. D. A lack of physical security could allow a hacker to plant a rogue wireless access point on the network.

20. A. Unauthorized personnel recorded on a security camera is an indication of a physical site security breach.