Chap_2_3AB_2026

1. A school notices a laptop went missing overnight. How could a properly used security camera help detect what happened?

A. Cameras delete evidence to protect privacy.

B. Cameras prevent all hacking attempts on Wi-Fi.

C. Recorded and monitored footage can show who entered and what they did, helping identify the theft.

D. Cameras automatically lock all doors when a laptop is moved.

2. Why is recording a camera feed important for physical security?

A. Recording replaces the need for any other controls.

B. Recording makes the camera's image brighter.

C. Recording forces attackers to leave immediately.

D. Recordings provide evidence that can be reviewed during and after an incident.

3. A company installs cameras but does not record or monitor them. Why is this less effective for detecting physical attacks?

A. Without monitoring or recordings, suspicious activity may be missed and evidence may be unavailable later.

B. Cameras only detect malware, not people.

C. Cameras only work if they are wireless.

D. Cameras cannot capture video unless the lights are off.

4. A camera shows an unknown person entering a badge-only door by slipping in behind an employee. Which physical attack does this evidence support?

A. Strong authentication

B. Tailgating

C. Software patching

D. Dumpster diving

5. Security footage shows a person asking someone to hold the door because they 'forgot their badge,' then entering a restricted area. What attack is most likely?

A. Data backup

B. Shoulder surfing

C. Card encryption

D. Piggybacking

6. Which camera setup would best maximize detection of suspicious hallway access?

A. A camera pointed at the floor with no recording

B. A camera that takes one photo per day

C. A camera with recording turned off to save storage

D. A camera that is monitored and records the entry area continuously

7. How can security guards help detect physical attacks in a building?

A. They automatically patch operating systems.

B. They replace the need for any doors or locks.

C. They encrypt all files on computers.

D. They can observe activity, identify suspicious behavior, and respond when something looks wrong.

8. A guard sees someone trying multiple doors late at night and reports it. How does this detect a possible physical attack?

A. The guard deletes system logs to hide the event.

B. The guard identifies unusual behavior and alerts others before damage or theft occurs.

C. The guard increases internet speed to stop the attacker.

D. The guard changes firewall rules to block the person.

9. A guard reports an unknown person wearing a fake maintenance badge near the server room. Which type of attack is the guard most likely detecting?

A. Social engineering to gain physical access

B. Password hashing

C. ARP spoofing

D. SQL injection

10. Why can guards be more effective than cameras in some situations?

A. Guards can store unlimited video recordings.

B. Guards automatically stop power outages.

C. Guards can remotely update all devices at once.

D. Guards can respond immediately when they notice suspicious activity.

11. A company has cameras, but no one watches them live. What additional benefit do guards add for detection?

A. They provide real-time monitoring and can investigate alerts right away.

B. They guarantee that no one will ever attempt entry.

C. They make camera images higher resolution.

D. They replace the need for recordings.

12. How do motion sensors help detect physical attacks?

A. They send an alert when movement is detected in an area.

B. They update antivirus definitions automatically.

C. They lock user accounts after failed logins.

D. They convert passwords into encryption keys.

13. A storage room should be empty after 7 p.m. A motion sensor triggers at 9 p.m. Why is this useful for detection?

A. It proves the building is safe because something moved.

B. It automatically identifies the attacker's name.

C. It signals unexpected movement, which can indicate unauthorized access.

D. It stops all devices from connecting to Wi-Fi.

ANS: C

14. Which placement would best help a motion sensor detect break-ins?

A. In a classroom during scheduled class time only

B. Near entry points and inside restricted rooms where no one should be moving after hours

C. Behind a computer monitor facing the wall

D. Inside a locked desk drawer

15. A motion sensor alert is followed by camera footage of someone opening a server cabinet. What does combining these controls help you do?

A. Confirm the alert was real and gather evidence of the physical attack

B. Encrypt the entire network instantly

C. Guarantee the attacker's device is infected with malware

D. Automatically restore deleted files

16. Why might motion sensors reduce the time it takes to detect an intrusion?

A. They stop all physical attacks from happening.

B. They can trigger immediate alerts instead of waiting for someone to notice the intrusion later.

C. They require no electricity to work.

D. They only detect floods and earthquakes.

17. Why are employees often the first to detect an unauthorized person in a workplace?

A. They can automatically disable door locks.

B. They can see through walls using special equipment.

C. They can scan fingerprints without tools.

D. They notice people who do not belong and can report concerns quickly.

18. An employee sees an unknown person in a restricted hallway and calls security. How does this support detection?

A. It creates a timely alert based on human observation of unusual access.

B. It changes IP addresses to block the person.

C. It resets the building's power system.

D. It prevents software bugs from happening.

19. An employee reports someone watching them type a door code. Which physical attack is the employee likely detecting?

A. MAC flooding

B. DNS spoofing

C. Shoulder surfing

D. Data compression

20. Which policy best supports employees as a detection control?

A. Allowing everyone to enter any room without badges

B. Turning off all alerts to avoid distractions

C. Clear instructions for reporting unknown people and suspicious behavior

D. Sharing door codes publicly to save time

21. Why is employee reporting considered a security control even though it is not a device?

A. It makes passwords unnecessary.

B. It replaces encryption for stored data.

C. It prevents all power failures.

D. It is a method of monitoring physical spaces that can trigger a response to suspicious activity.

22. A school wants to maximize the usefulness of its cameras. Which approach best explains what to do and why?

A. Turn cameras off at night to protect privacy.

B. Use cameras only during fire drills to save storage.

C. Point cameras at the ceiling so they are harder to find.

D. Record and monitor the feed so suspicious actions are noticed and evidence is saved for investigations.

23. A guard notices a person repeatedly trying to enter a badge-only door and then leaving quickly. Why is this considered detection?

A. The guard prevented all future break-ins automatically.

B. The guard changed the device's password remotely.

C. The guard identified suspicious behavior that could signal an attempted unauthorized entry.

D. The guard improved the door's encryption.

24. A motion sensor triggers in a server room, but a quick camera check shows a janitor cleaning with permission. What does this show about detection controls?

A. Cameras can only be used after an arrest.

B. Alerts can identify unusual activity, and evidence can be used to confirm whether it is a real incident.

C. Motion sensors always mean an attack occurred.

D. Employees should ignore all alerts.

25. Which situation best shows employees detecting a physical breach?

A. A firewall blocks an incoming packet

B. A staff member recognizes an unfamiliar person in a restricted area and reports it

C. A router changes its routing table

D. An antivirus scan deletes a file

26. After a break-in, investigators review recorded camera footage and see someone connect a USB drive to a workstation. What does the footage help confirm?

A. The attacker used only remote access

B. The workstation automatically updated correctly

C. A physical attack occurred and may have introduced malicious hardware or malware

D. The network became faster during the incident

27. A guard finds an unknown device plugged into a public kiosk's USB port and reports it. Which type of incident is most likely being detected?

A. A software patch failure

B. A DDoS attack against a website

C. A DNS resolution error

D. A physical attempt to load malware or capture data via an external device

28. Why is it useful to pair motion sensors with cameras for detection?

A. Motion sensors can store video better than cameras.

B. Using both guarantees no one can enter.

C. Sensors can alert quickly, and cameras can provide visual evidence of what triggered the alert.

D. Cameras cannot record without motion sensors.

29. An employee reports seeing someone take photos of a badge reader while standing very close. Which physical attack might this evidence suggest?

A. MAC spoofing

B. Packet sniffing

C. Brute force password cracking

D. An attempt to capture access information through observation (shoulder surfing)

30. Which statement best explains why camera recordings are especially helpful after an incident?

A. They automatically restore damaged devices.

B. They provide evidence that can be reviewed to understand what happened and support investigations.

C. They permanently block all visitors.

D. They change building locks to new codes.

31. A guard responds to a motion alert and finds a door propped open. How do the controls work together to detect the issue?

A. The sensor disables the building’s power.

B. The guard encrypts the sensor’s data to stop the alert.

C. The sensor detects movement and the guard verifies and responds to the suspicious condition.

D. The camera updates the guard’s password automatically.

32. A school wants to identify who enters through a side door after hours. Where should a camera be placed for the most useful evidence?

A. Inside a locked drawer in the office

B. In the center of the gym aimed at the ceiling

C. Above the side door, aimed to capture faces and the door handle area

D. Behind a computer monitor facing the wall

33. A data center has one main entry and two emergency exits. Which locations are most important to monitor with cameras?

A. Only the break room

B. Points of ingress and egress such as the main entry and emergency exits

C. Only the server rack interiors

D. Only the parking spaces far from the building

34. A camera is installed at an entrance but can easily be reached and covered by someone standing on a chair. What placement improvement best reduces tampering?

A. Mount the camera higher and out of easy reach while keeping a clear view of the doorway

B. Turn off recording to save storage

C. Point the camera at the floor to avoid privacy issues

D. Move the camera to the cafeteria

35. A store wants a camera to capture what an adversary does at the cash office door (e.g., trying handles or forcing entry). What placement is best?

A. Angle the camera to include the door, lock, and the person’s hands

B. Aim the camera at the parking lot across the street

C. Place the camera inside the cash drawer

D. Point the camera only at the hallway ceiling lights

36. A school has a camera at the main entrance, but it only captures the backs of people entering. What is the best adjustment?

A. Lower the camera until it is at waist height

B. Turn the camera off during the day

C. Move the camera to the teacher lounge

D. Reposition the camera to capture faces as people enter and exit

37. Which camera placement best balances visual coverage and useful evidence for investigations?

A. A camera in the restroom entrance

B. A camera at the door with a wide view plus a second camera down the hall to track movement

C. One camera in the server room pointed at a blank wall

D. A camera in a closet that is usually closed

38. Camera footage shows an unknown person avoiding the main entrance and entering through a rear door with a broken latch. What does this evidence suggest about camera placement?

A. Cameras should be placed only in high-traffic classrooms

B. Only interior hallways need cameras

C. Rear doors (ingress/egress) should also be monitored to capture alternate entry attempts

D. Cameras should never be placed near doors

39. A company can afford only one camera for a small office. Which location is most effective for detecting unauthorized entry?

A. In a storage room used once per month

B. The main entrance where most people must pass

C. Inside a locked filing cabinet

D. On a desk facing the wall

40. Where should motion sensors be placed to reduce false alarms and detect real intrusions?

A. At the front of every classroom during class

B. In low-traffic sensitive areas like server rooms and storage rooms for secure materials

C. In the main hallway during class changes

D. In the cafeteria at lunch

41. A hospital placed motion sensors in a busy lobby and now receives constant alerts. What is the main problem with this placement?

A. Motion sensors delete camera recordings

B. High traffic creates many false alarms, so real events may be ignored

C. Motion sensors stop power outages

D. Motion sensors only work outdoors

42. A school wants a motion sensor to detect after-hours entry into the network closet. What placement is best?

A. Inside the network closet where movement is unexpected after hours

B. In the main office during the school day

C. In the gym during practice

D. Outside the building facing the street

43. A business stores backup drives in a secure cabinet inside a rarely used room. Where is the best place for a motion sensor?

A. In the room near the cabinet to detect unexpected movement

B. In the parking lot where cars pass frequently

C. In the open-plan workspace where employees move all day

D. In the break room near the vending machines

44. After multiple false alarms, staff stop responding quickly. Later, a real break-in occurs and the alert is ignored. What does this show?

A. Cameras always cause false alarms

B. Motion sensors should never be used

C. Locks are only useful for laptops

D. Placing sensors in high-traffic areas can reduce effectiveness because alarms lose credibility

45. Which location is least appropriate for a motion sensor if the goal is to detect

intrusions?

A. A server room with limited access

B. A hallway used by hundreds of students every hour

C. A storage room for sensitive files

D. A restricted lab after hours

46. A company wants to detect access to a safe where sensitive paper files are stored. The room is usually empty. What control placement is best?

A. A motion sensor in the file room near the safe

B. A motion sensor in the cafeteria

C. A guard stationed inside a supply closet

D. A camera pointed at the parking lot only

47. What is the best reason to avoid motion sensors in high-traffic areas?

A. High traffic improves detection accuracy

B. Too many alerts can cause people to ignore alarms during real events

C. High traffic makes devices run slower

D. Sensors will stop working permanently

48. A company keeps payroll records on a server in a room with no lock. What is the most effective placement decision?

A. Put a lock on the office trash can

B. Install a lock on the server room entry door

C. Add a camera facing the parking lot

D. Install a motion sensor in the cafeteria

49. A lab has very sensitive systems and has a problem with piggybacking at the door. Which placement of a control is most effective?

A. Place cameras only inside the lab, away from the door

B. Move the lab computers to a different desk

C. Install a motion sensor in the hallway outside the building

D. Install an access control vestibule at the lab entry point

50. Which area should have locks on all entries according to best practice in this topic?

A. Only outdoor sidewalks

B. Any area that stores snacks

C. Areas containing sensitive information or systems

D. Only public lobbies

51. A school stores standardized test materials in a supply closet. Only two staff members should access it. What is the best control placement?

A. Place a camera in the gym

B. Install a lock on the closet door and control who has keys or access

C. Disable Wi-Fi in the school

D. Install a motion sensor in the main hallway

52. An entry log shows multiple instances where two people enter on one badge swipe. What vulnerability does this evidence most likely indicate?

A. Piggybacking at a controlled entry point

B. Dumpster diving

C. Phishing

D. Malware patching

53. A business has locks on the server room door, but the side door to the same room is propped open for deliveries. What placement change is most important?

A. Move the server to a higher shelf

B. Ensure all entries to the sensitive area are secured with locks and not left propped open

C. Add more posters about safety

D. Turn off camera recording to save space

54. For a highly sensitive area, which combination best prevents piggybacking at the entry?

A. Only a privacy screen on monitors

B. Only a motion sensor in the cafeteria

C. Locks plus an access control vestibule at the entrance

D. Only disabling USB ports

55. A museum has one main lobby that all visitors must pass through. Where is a stationary guard placement most effective?

A. At a random hallway that few people use

B. At the main lobby entrance where traffic funnels

C. On the roof away from entrances

D. Inside a locked closet

56. A warehouse has a large perimeter and several exterior doors. Which guard strategy best increases detection and creates time pressure for an adversary?

A. Use no guards and rely only on signs

B. Use patrolling guards only inside a locked office

C. Use only one stationary guard in the break room

D. Use patrolling guards around the perimeter and exterior areas

57. Why are patrolling guards harder for an adversary to plan around?

A. They can read encrypted files

B. They can disable all motion sensors

C. They reduce the need for locks

D. Their routes and timing are less predictable, creating uncertainty for the adversary

58. A bank wants constant protection for an ATM room and wants to deter tampering. Which placement is best?

A. A patrolling guard only outside the city

B. A camera pointed at the parking lot only

C. A stationary guard near the ATM room entrance

D. A motion sensor in the cafeteria

59. A guard report notes repeated suspicious activity at an entry gate at 2 a.m. over several nights. Which placement decision is most supported by this evidence?

A. Remove all cameras from the entry gate

B. Move motion sensors to the busiest hallway

C. Unlock side doors to reduce congestion

D. Place a stationary guard at the entry gate where traffic funnels

60. A stadium has multiple exterior access points. Which combination of guard placements is most effective?

A. Only stationary guards in a storage closet

B. Stationary guards at main entrances and patrolling guards on the exterior perimeter

C. No guards, only door mats

D. Only patrolling guards inside the stadium offices

61. A company has a high-value prototype stored in a display room. What guard placement best provides constant protection for that specific item?

A. A patrolling guard who never goes near the display room

B. A stationary guard assigned to the display room

C. A camera that is not recorded

D. A motion sensor in the parking lot

62. A school wants to detect people leaving through emergency exits with stolen devices. Where should cameras be placed for this goal?

A. Only in the teacher lounge

B. Only in classrooms

C. At emergency exits to capture egress and evidence of stolen items

D. Only in the cafeteria

63. A company is choosing between placing a motion sensor in a server room or in a busy open office. Which placement is more effective and why?

A. Server room, because unexpected movement there is meaningful and reduces false alarms

B. Either location is the same

C. Open office, because more people create more alerts

D. Open office, because false alarms are helpful

64. A research lab has sensitive systems and frequent visitors. Which entry control

placement best reduces risk from piggybacking?

A. A lock only on the lab’s filing cabinet

B. A motion sensor in the lobby

C. An access control vestibule at the lab entrance

D. A camera aimed at the ceiling

65. An organization wants to deter and detect suspicious activity at the main lobby and also watch the exterior at night. Which guard placement plan best fits?

A. Only stationary guards on the perimeter

B. Only patrolling guards in the lobby

C. No guards; only signs and posters

D. Stationary guard in the main lobby and patrolling guards on exterior areas

66. Camera footage shows an attacker covering a camera with tape before entering a restricted room. What placement factor was most likely overlooked?

A. The camera’s ability to be tampered with by an adversary

B. The type of Wi-Fi encryption used

C. The number of students in the building

D. The color of the camera housing