

Exercise walk-through

2.3

Protecting Physical Spaces

AP Cybersecurity

Physical attacks – walking straight in

Digital security means nothing if an adversary can simply walk in. Most **physical attacks** begin with **social engineering**:

Piggybacking

()
the authorised person
holds the door – tricked

Tailgating

()
slipping through unnoticed

Shoulder surfing

watching you type

Dumpster diving

ing
card cloning ■

Piggybacking has consent (you were tricked); tailgating does not (you never knew). The exam tests this exact pair.

Protecting physical spaces

Managerial first: security-awareness training (do not badge strangers in) and a workstation policy – locking devices, a **clean desk policy**, privacy screens.

With physical access an adversary can cut power, copy data, or plug in a **key-logger**.

fences, gates, **bol-lards** – deter

card readers
– log and restrict

access control vestibule
– stops piggybacking

disabled USB ports;
a **UPS**

Detecting physical attacks – placement matters

Some controls **detect** rather than prevent: cameras record, guards respond, **motion sensors** alert – and **employees** often notice an intruder first.

Cameras belong at **points of ingress and egress**.

Motion sensors work in low-traffic areas like server rooms. Put one in a busy hallway and the constant false alarms make everyone ignore them.

A stationary guard protects a fixed high-value point; a patrolling guard is harder to plan around. Reviewing door-open times can reveal piggybacking – a door held open too long is suspicious.

Protecting Physical Spaces, continued



A dome security camera: physical controls and monitoring protect spaces as well as networks

Cyber Foundations



A monitor wall: network monitoring and logging help detect intrusions

Exercises 2.1-2.2

2.1 State **two** managerial controls related to physical security and explain what each does. [4]

2.2 Explain why a workstation security policy may have **tiers**. [2]

Exercises 2.1-2.2

2.1 State **two** managerial controls related to physical security and explain what each does. [4]

2.1

- **security awareness training** - educates employees about how they can contribute to the organisation's security; a **workstation security policy** - outlines the measures necessary to protect a physical workplace

2.2 Explain why a workstation security policy may have **tiers**. [2]

2.2

- different areas carry different sensitivity, so tiers let the policy set stricter requirements for a records office or laboratory than for a public reception desk, instead of forcing one standard that is either too weak or unworkably strict

Exercise 2.3 (a)

2.3 Name the physical control that best addresses each vulnerability.

(a) An adversary can walk in behind an authorised employee.

[1]

Exercise 2.3 (a)

2.3 Name the physical control that best addresses each vulnerability.

(a) An adversary can walk in behind an authorised employee.

[1]

(a)

- an access control vestibule or turnstile

Exercise 2.3 (b)

2.3 Name the physical control that best addresses each vulnerability.

(b) Malware could be loaded from an external drive at an unattended machine. [1]

Exercise 2.3 (b)

2.3 Name the physical control that best addresses each vulnerability.

(b) Malware could be loaded from an external drive at an unattended machine. [1]

(b)

- disabled USB ports

Exercise 2.3 (c)

2.3 Name the physical control that best addresses each vulnerability.

(c) The building's services stop whenever the mains supply fails.

[1]

Exercise 2.3 (c)

2.3 Name the physical control that best addresses each vulnerability.

(c) The building's services stop whenever the mains supply fails.

[1]

(c)

- a UPS, or a power generator

Exercise 2.3 (d)

2.3 Name the physical control that best addresses each vulnerability.

(d) There is no record of who entered the records office last night.

[1]

Exercise 2.3 (d)

2.3 Name the physical control that best addresses each vulnerability.

(d) There is no record of who entered the records office last night.

[1]

(d)

- a card reader

Exercise 2.3 (e)

2.3 Name the physical control that best addresses each vulnerability.

(e) A server could be carried out of an open rack.

[1]

Exercise 2.3 (e)

2.3 Name the physical control that best addresses each vulnerability.

(e) A server could be carried out of an open rack.

[1]

(e)

- a lock on the server cabinet

Exercises 2.4-2.5

2.4 Explain why an access control vestibule addresses tailgating when a card reader alone does not. [3]

2.5 State the **two** things a card reader does. [2]

Exercises 2.4-2.5

2.4 Explain why an access control vestibule addresses tailgating when a card reader alone does not. [3]

2.4

- a card reader denies unauthorised badges and records which badge opened the door, but once the door is open it cannot tell how many people pass through; a vestibule or turnstile physically admits one person at a time, so an unauthorised follower is stopped whether the authorised person intended to admit them or not

2.5 State the **two** things a card reader does. [2]

2.5

- it records which employee badges are used to access which entries at what times; and it denies access to unauthorised badges

Exercises 2.6-2.7

2.6 Explain why security awareness training is the control that addresses piggybacking.[2]

2.7 State what a **UPS** provides and give one situation where a generator is needed instead. [2]

Exercises 2.6-2.7

2.6 Explain why security awareness training is the control that addresses piggybacking.[2]

2.6

- in piggybacking the authorised person **chooses** to grant access, so no physical control at that door is engaged; training is what equips the employee to recognise the manipulation and refuse, which is the only point at which that attack can be stopped

2.7 State what a **UPS** provides and give one situation where a generator is needed instead. [2]

2.7

- a UPS provides a backup power source for a device during a power outage, keeping it and its services available; a generator is needed for a long outage, because a UPS holds a device up only for a limited period

Exercise 2.8 (a)

2.8 An organisation has two proposed mitigations: a \$200 policy of shredding confidential waste, closing a route that has already leaked customer data; and a \$60,000 perimeter fence around a car park where nothing sensitive is stored.

(a) State the two factors used to prioritise mitigations.

[2]

Exercise 2.8 (a)

2.8 An organisation has two proposed mitigations: a \$200 policy of shredding confidential waste, closing a route that has already leaked customer data; and a \$60,000 perimeter fence around a car park where nothing sensitive is stored.

(a) State the two factors used to prioritise mitigations. [2]

(a)

- the severity of the risks and the cost of the recommended mitigations

Exercise 2.8 (b)

2.8 An organisation has two proposed mitigations: a \$200 policy of shredding confidential waste, closing a route that has already leaked customer data; and a \$60,000 perimeter fence around a car park where nothing sensitive is stored.

(b) State which you would implement first and justify it.

[2]

Exercise 2.8 (b)

2.8 An organisation has two proposed mitigations: a \$200 policy of shredding confidential waste, closing a route that has already leaked customer data; and a \$60,000 perimeter fence around a car park where nothing sensitive is stored.

(b) State which you would implement first and justify it. [2]

(b)

- the **shredding policy** - it costs almost nothing and closes a route that has already caused a real leak of customer data, whereas the fence is 300 times the cost and protects a car park holding nothing sensitive, so the severity-to-cost ratio is far worse

Exercises 3.1-3.2

3.1 Which control best prevents an authorised person from admitting an unauthorised one? [1]

☐

- A** a card reader
- B** an access control vestibule
- C** a bollard
- D** a server cabinet lock

3.2 Disabling USB ports on a workstation primarily prevents [1]

☐

- A** tailgating
- B** an external drive loading malware onto the computer
- C** shoulder surfing
- D** power disruption

Exercises 3.1-3.2

3.1 Which control best prevents an authorised person from admitting an unauthorised one? [1]

- ☐ **A** a card reader
B an access control vestibule
C a bollard
D a server cabinet lock

3.1 B

- That is the vestibule's defining purpose, including accidental admission

3.2 Disabling USB ports on a workstation primarily prevents [1]

- ☐ **A** tailgating
B an external drive loading malware onto the computer
C shoulder surfing
D power disruption

3.2 B

- an external drive loading malware onto the computer.

Exercises 3.3-3.4

3.3 A UPS protects mainly against a loss of

[1]

☐

A confidentiality

B integrity

C availability

D authenticity

3.4 Organisations prioritise risk mitigations based on

[1]

☐

A severity of the risks and cost of the mitigations

B the order in which vulnerabilities were discovered

C the number of employees affected

D whether the control is physical or managerial

Exercises 3.3-3.4

3.3 A UPS protects mainly against a loss of

[1]

☐

- A confidentiality
- B integrity
- C availability
- D authenticity

3.3 C

- A power outage makes the device and its services unavailable

3.4 Organisations prioritise risk mitigations based on

[1]

☐

- A severity of the risks and cost of the mitigations
- B the order in which vulnerabilities were discovered
- C the number of employees affected
- D whether the control is physical or managerial

3.4 A

- severity of the risks and cost of the mitigations.

Exercise 3.5 (a)

3.5 A regional blood bank has a laboratory holding donor records and refrigerated stock, reached from a staffed reception through one card-reader door. Deliveries arrive at a rear door that staff prop open during the morning round. Freezers and the record server share the mains supply with the rest of the building. Staff have received no security training; last month a courier was let into the laboratory because “he had a clipboard and was in a hurry”.

(a) Identify **three** vulnerabilities and, for each, name the attack an adversary could use.[6]

Exercise 3.5 (a)

3.5 A regional blood bank has a laboratory holding donor records and refrigerated stock, reached from a staffed reception through one card-reader door. Deliveries arrive at a rear door that staff prop open during the morning round. Freezers and the record server share the mains supply with the rest of the building. Staff have received no security training; last month a courier was let into the laboratory because “he had a clipboard and was in a hurry”.

(a) Identify **three** vulnerabilities and, for each, name the attack an adversary could use.[6]

(a)

- any three, each with an attack: the **propped rear door** - tailgating, or simple unauthorised entry; **no security awareness training** - piggybacking, as already demonstrated by the courier; a **single card-reader door** with no vestibule - tailgating behind a staff member; **shared mains supply** with no backup - power disruption causing loss of availability

Exercise 3.5 (b)

3.5 A regional blood bank has a laboratory holding donor records and refrigerated stock, reached from a staffed reception through one card-reader door. Deliveries arrive at a rear door that staff prop open during the morning round. Freezers and the record server share the mains supply with the rest of the building. Staff have received no security training; last month a courier was let into the laboratory because “he had a clipboard and was in a hurry”.

(b) Recommend a control for each vulnerability you named, showing the reasoning from attack to control.

[6]

Exercise 3.5 (b)

3.5 A regional blood bank has a laboratory holding donor records and refrigerated stock, reached from a staffed reception through one card-reader door. Deliveries arrive at a rear door that staff prop open during the morning round. Freezers and the record server share the mains supply with the rest of the building. Staff have received no security training; last month a courier was let into the laboratory because “he had a clipboard and was in a hurry”.

(b) Recommend a control for each vulnerability you named, showing the reasoning from attack to control. [6]

(b)

- a control for each, with the reasoning shown. For example: an adversary could walk through the propped rear door unchallenged, so fit a self-closing door with a card reader, and provide a bell for deliveries (attack control);
- an adversary could talk a member of staff into admitting them, so run security awareness training that covers piggybacking and gives staff a script for refusing (attack control);
- an adversary could follow a member of staff through the card-reader door, so install a vestibule or turnstile admitting one person at a time (attack control);
- control)

Exercise 3.5 (c)

3.5 A regional blood bank has a laboratory holding donor records and refrigerated stock, reached from a staffed reception through one card-reader door. Deliveries arrive at a rear door that staff prop open during the morning round. Freezers and the record server share the mains supply with the rest of the building. Staff have received no security training; last month a courier was let into the laboratory because “he had a clipboard and was in a hurry”.

(c) Explain the specific consequence of a power outage here, and name the control that addresses it. [3]

Exercise 3.5 (c)

3.5 A regional blood bank has a laboratory holding donor records and refrigerated stock, reached from a staffed reception through one card-reader door. Deliveries arrive at a rear door that staff prop open during the morning round. Freezers and the record server share the mains supply with the rest of the building. Staff have received no security training; last month a courier was let into the laboratory because “he had a clipboard and was in a hurry”.

(c) Explain the specific consequence of a power outage here, and name the control that addresses it. [3]

(c)

- a power outage makes the record server and its services unavailable, and here it also stops the refrigeration, so the blood stock itself is at risk of destruction - a loss far beyond the IT systems. The control is a **UPS**, with a **generator** for a sustained outage given how long refrigeration must be maintained

Exercise 3.5 (d)

3.5 A regional blood bank has a laboratory holding donor records and refrigerated stock, reached from a staffed reception through one card-reader door. Deliveries arrive at a rear door that staff prop open during the morning round. Freezers and the record server share the mains supply with the rest of the building. Staff have received no security training; last month a courier was let into the laboratory because “he had a clipboard and was in a hurry”.

(d) The blood bank can fund only two mitigations this year. State which two you would choose and justify the choice against both prioritisation factors. [4]

Exercise 3.5 (d)

3.5 A regional blood bank has a laboratory holding donor records and refrigerated stock, reached from a staffed reception through one card-reader door. Deliveries arrive at a rear door that staff prop open during the morning round. Freezers and the record server share the mains supply with the rest of the building. Staff have received no security training; last month a courier was let into the laboratory because “he had a clipboard and was in a hurry”.

(d) The blood bank can fund only two mitigations this year. State which two you would choose and justify the choice against both prioritisation factors. [4]

(d)

- Any two defensible choices, justified against **both** factors. Strongest answer: **security awareness training**, because it is inexpensive and addresses the attack that has already succeeded here; and **a UPS and generator for the refrigeration and server**, because although it is the most expensive item, the severity is the destruction of the blood stock itself, which no other mitigation on the list comes near

Exercise 3.5 (e)

3.5 A regional blood bank has a laboratory holding donor records and refrigerated stock, reached from a staffed reception through one card-reader door. Deliveries arrive at a rear door that staff prop open during the morning round. Freezers and the record server share the mains supply with the rest of the building. Staff have received no security training; last month a courier was let into the laboratory because “he had a clipboard and was in a hurry”.

(e) The director argues training is “the cheapest control, so it should always come first”. Evaluate this. [3]

Exercise 3.5 (e)

3.5 A regional blood bank has a laboratory holding donor records and refrigerated stock, reached from a staffed reception through one card-reader door. Deliveries arrive at a rear door that staff prop open during the morning round. Freezers and the record server share the mains supply with the rest of the building. Staff have received no security training; last month a courier was let into the laboratory because “he had a clipboard and was in a hurry”.

(e) The director argues training is “the cheapest control, so it should always come first”. Evaluate this. [3]

(e)

- Partly right, and incomplete. Training is inexpensive and it is the only control that reaches social engineering, so on the severity-to-cost ratio it very often does come first. But cost is only one of the two factors - if a cheap control addresses a low-severity risk while an expensive one prevents the destruction of the blood stock, the expensive one wins; and training does not close a propped door or keep a freezer running, so it can never be a complete answer on its own