

2.3 Protecting Physical Spaces

Name: _____ Class: _____ Date: _____ **Total: 50 marks**

KEY WORDS ups 不间断电源 • managerial 管理 • access control vestibule 门禁前室
• physical controls 物理控制 • card readers 读卡器

Objective

Build the skills to answer exam questions on **managerial** 管理 and **physical controls** 物理控制 for physical security, and on prioritising mitigations.

You must be able to:

- describe security awareness training and a workstation security policy, and say why each is managerial
- match a physical control to the vulnerability it addresses
- explain how the cyber defender reasons from attack to control
- explain what a **UPS** 不间断电源 and a generator protect against
- prioritise mitigations by severity of risk against cost

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ The two managerial controls

A managerial control provides rules, guidelines, policies and procedures - it does not itself stop anybody.

- **Security awareness training** educates employees about how they contribute to the organisation's security. It is the only control that reaches the vulnerability social engineering exploits, because that vulnerability is a *person*. A lock does not help when the employee opens the door themselves.
- **A workstation security policy** sets out the measures needed to protect a physical workplace, and it may have **tiers** - different requirements for areas of different sensitivity, so a public reception desk and a records office are not held to one standard.

■ How a defender chooses a control

The reasoning runs in one direction, and questions ask you to show it:

How could an adversary **take advantage of this vulnerability** to attack the system, and how do I **prevent that specific route**?

So name the attack first, then the control that blocks it. A control offered without the attack it prevents is an unjustified guess.

■ The physical controls and what each addresses

Control	The route it closes
Fencing, gates, bollards	deter an adversary from approaching the building at all
Locks on doors, server cabinets, computers	prevent devices being accessed or stolen
Card readers	deny unauthorised badges, and record which badge entered where and when
Access control vestibules, turnstiles	prevent an authorised person admitting an unauthorised one - intentionally or accidentally
Disabled USB ports	prevent an external drive loading malware onto a computer
UPS, power generators	keep devices running through a power outage

Two of these deserve special attention because they answer questions the others cannot.

A vestibule or turnstile is the control for tailgating and piggybacking, and it is the only one on the list that is: a lock does not help when the door is already open for the authorised person, and a card reader records the badge that opened it but not the second person who walked through.

A card reader's logging is half its value. It denies unauthorised badges *and* creates the record that lets an investigator reconstruct who entered a restricted area and when - a detective function on top of a preventative one.

A UPS answers the natural-disaster and power-disruption half of the threat model. It provides backup power during an outage, so a device and its services stay available; a generator extends that to a long outage.

■ Prioritising

Organisations prioritise mitigations by **the severity of the risks** against **the cost of the recommended mitigations**. So the first thing to fix is not the worst vulnerability but the best **ratio**: a cheap control closing a severe route beats an expensive control closing a minor one. Say both halves when you justify an order.

2 Practice

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]

2.3 Name the physical control that best addresses each vulnerability.

- (a) An adversary can walk in behind an authorised employee. [1]
- (b) Malware could be loaded from an external drive at an unattended machine. [1]
- (c) The building's services stop whenever the mains supply fails. [1]
- (d) There is no record of who entered the records office last night. [1]
- (e) A server could be carried out of an open rack. [1]

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]

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]

2.8 An organisation has two proposed mitigations: a 200*policy of shredding confidential waste, closing a* perimeter fence around a car park where nothing sensitive is stored.

- (a) State the two factors used to prioritise mitigations. [2]
- (b) State which you would implement first and justify it. [2]

3 Exam-style questions

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

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

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]

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

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

(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]

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

Solutions

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 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.

2.3 (a) an access control vestibule or turnstile. (b) disabled USB ports. (c) a UPS, or a power generator. (d) a card reader. (e) a lock on the server cabinet.

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

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 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.

2.8 (a) the severity of the risks and the cost of the recommended mitigations. (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.

3.1 B. That is the vestibule's defining purpose, including accidental admission.

3.2 B.

3.3 C. A power outage makes the device and its services unavailable.

3.4 A.

3.5 (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.

(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).

(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.

(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.

(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.