

Solutions

Each answer shows the steps, then the **result**.

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