

Solutions

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

2.1

(a)

- piggybacking

(b)

- tailgating

(c)

- shoulder surfing

(d)

- dumpster diving

(e)

- card cloning

2.2

- in **piggybacking** the adversary uses social engineering to persuade an authorised person to **grant** them access, so the person knowingly lets them in; in **tailgating** the adversary simply follows close behind an authorised person, who does not know they are there

2.3

- unauthorised access to sensitive data or restricted physical spaces; disruption of services; theft or destruction of digital or physical resources; unauthorised modification of data

2.4

- threats include natural disasters as well as human adversaries; a flood or fire can physically damage or destroy the assets themselves, causing the same loss of availability an attacker would - so physical security must plan for both

2.5

(a)

- the device and every service it provides become unavailable - a denial of service achieved without touching the network at all

(b)

- they can plug in a keylogger, capturing everything the user types including passwords, or an external drive carrying malware which the device may run

(c)

- they can steal or copy the sensitive information, an unauthorised access to sensitive data that leaves the computer systems entirely untouched

2.6

- physical access lets an adversary bypass many technical controls and layers of security - a firewall cannot filter a person standing at the machine, and an access control model does not apply once the device has been booted another way or its drive removed

2.7

(a)

- **high** - sensitive systems holding financial records are exposed in a space that is neither sufficiently restricted nor monitored

(b)

- **moderate** - a non-critical, non-sensitive part of the organisation left unprotected in a way that could be exploited; accept low with justification about asset value

(c)

- **low** - the asset is of low value and, with a staffed reception, exploitation is unlikely

3.1 B

- The employee grants the access, which is what separates piggybacking from tailgating

3.2 C

3.3 B

3.4 B

- A and C are moderate; D is high

3.5

(a)

- any three, each with its enabling feature: **piggybacking** - the stranger asking staff to hold the office door; **tailgating** - a card-reader door in a public building through which anyone may follow; **dumpster diving** - borrower record drafts recycled in an open bin; **shoulder surfing** - staff working on borrower records in an area the public can see; **card cloning** - staff badges carried openly in a public space

(b)

- an adversary in the comms cupboard has physical access to network devices and their ports. Two distinct compromises, any two: **disruption of services** by cutting power or unplugging equipment, making the library's systems unavailable; **unauthorised access** by plugging into a data port or installing a rogue access point, giving a route

onto the internal network; **theft or destruction** of the equipment itself. Maximum
4

(c)

- The reasoning is **wrong**. The compromise defined by the course is unauthorised access to **sensitive data**, and the format of that data is irrelevant - names, addresses and fine histories are personal data whether printed or stored. Dumpster diving is a named attack precisely because paper is often the easiest route to information that is well protected digitally, and it needs no technical skill at all

(d)

- **High**. Sensitive borrower information is exposed in physical spaces that are not sufficiently restricted or monitored - the open recycling bin, the visible screens; and the propped comms cupboard gives physical access to network equipment in a public corridor, which bypasses whatever technical controls the library has

(e)

- Three controls, each on a different attack: a shredder or locked confidential-waste bin for borrower drafts; a self-closing lock and ventilation fix so the comms cupboard cannot be propped; an access control vestibule or turnstile, plus security-awareness training so staff are equipped to refuse the door request; privacy screens or repositioned monitors. First: **secure the comms cupboard**, because physical access to network equipment bypasses every technical control at once and the door is currently open to the public. Accept the confidential-waste bin as first if justified by the ongoing, certain exposure of personal data