

Solutions

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

2.1

- confidentiality - only authorised people can read the data, e.g. encryption; integrity - the data is accurate and unaltered, e.g. a hash or checksum; availability - data and services are there when needed, e.g. a backup or redundant server. Accept any control that genuinely serves the named goal

2.2

(a)

- **scarcity** - “only three licences left” / “closes tonight” invents limited availability. Accept urgency as a second tactic if quoted from “closes tonight”

(b)

- **consensus** - “everyone else on your team has already” creates social pressure to conform

(c)

- **familiarity** - claiming a shared acquaintance, “we met at Priya’s leaving lunch”, to borrow trust. A bare label with no quotation scores 1 of 2

2.3

(a)

- hacktivist - motivated by a social or environmental cause, not money

(b)

- insider - holds legitimate credentials; motive is revenge

(c)

- transnational criminal organisation - ransomware for financial gain

(d)

- script kiddie - uses others’ tools without understanding them

2.4

(a)

- reconnaissance - public OSINT, still outside the system

(b)

- persistence - keeping access without regaining it

(c)

- evading detection

(d)

- taking action - exfiltrating the target data

2.5

- risk occurs when a threat can exploit a vulnerability to compromise an asset; any two non-physical assets, e.g. data, intellectual property, reputation, financial resources

2.6

(a)

- "likely, high impact" is qualitative; "\$40,000 expected annual loss" is quantitative

(b)

- any one of: it can be compared directly against the cost of a control, so the board can see whether a fix is cost effective; it can be added across risks into a budget; it removes the ambiguity of a word like "high"

2.7

(a)

- technical, preventative

(b)

- managerial, corrective - it restores operations after an incident; accept preventative only with a justification that it reduces damage before an incident

(c)

- physical, preventative

(d)

- technical, corrective

3.1 B

- Encryption hides the contents from anyone without the key, which is confidentiality

3.2 B

- Shifting the burden to another entity is transference. Note the loss of reputation does not transfer

3.3 C

- The foothold already exists, so this is not initial access; reaching further with higher privilege is lateral movement

3.4 B

- A SIEM identifies attacks as they occur. A bollard and encryption prevent; an IPS that blocks the connection is corrective

3.5

(a)

- **urgency** - “urgent regulator notice” imposes a deadline so the engineer acts before checking. Accept **authority** if the answer quotes the impersonation of a regulator

(b)

- **persistence**. The nightly call-out is a command-and-control channel, so the adversary keeps access without having to phish again, and can send new commands and retrieve output

(c)

- Likelihood **high** because: a water utility is a high-value target for a cyberterrorist or hostile state; a four-year-old shared password requires almost no skill to abuse; and the control network is reachable from the office network, so one phished user is enough. Severity **high** because: loss of availability at a treatment plant threatens public health, and the operational and reputational damage far exceeds the financial cost. Overall rating high/severe

(d)

- **Mitigate** - replace the shared password with individual accounts and multi-factor authentication, which cuts the likelihood at low cost. Avoidance is not possible because treating water is the utility’s purpose. Transference (insurance) does not stop the plant being taken offline and cannot restore public trust; acceptance is unjustifiable when severity is loss of safe water

(e)

- Defense in depth uses several controls of different types so that bypassing one still leaves others. Password policy defends the **human**/managerial layer; segmentation defends the **network** layer, so a phished office account no longer reaches the control system; the locked room defends the **physical** layer. Each threat meets the control best suited to it, and one failure no longer exposes the plant