

AP Cybersecurity

Name: _____ Score: _____

1. Encrypting data mainly protects which CIA goal?
 - ☐ Availability
 - ☐ Confidentiality
 - ☐ Integrity
 - ☐ Authority
2. Slipping through a secured door behind someone WITHOUT their knowledge is...
 - ☐ piggybacking
 - ☐ tailgating
 - ☐ shoulder surfing
 - ☐ card cloning
3. A two-door airlock that lets one person pass at a time is a(n)...
 - ☐ bollard
 - ☐ access control vestibule
 - ☐ UPS
 - ☐ card reader
4. Where are cameras most useful?
 - ☐ In empty storage closets
 - ☐ At points of ingress and egress
 - ☐ Facing a blank wall
 - ☐ Inside a locked safe
5. A risk exists when a threat exploits a _____ to harm an asset.
 - ☐ firewall
 - ☐ vulnerability
 - ☐ backup
 - ☐ policy
6. Defense in depth means using a single very strong control.
 - ☐ True ☐ False

7. Physical access to a device can let an adversary bypass many digital controls.

☐ True ☐ False

8. Security-awareness training is a managerial control.

☐ True ☐ False

9. A door that stays open unusually long can be a sign of piggybacking.

☐ True ☐ False

10. The leftover risk an organisation lives with after mitigation is _____ risk.

AP Cybersecurity

1. Confidentiality

Encryption hides data = **confidentiality**.

2. tailgating

Tailgating = unnoticed; **piggybacking** = with consent.

3. access control vestibule

An **access control vestibule** stops piggybacking.

4. At points of ingress and egress

Entrances and exits capture who comes and goes.

5. vulnerability

A **vulnerability** is the weakness a threat uses.

6. False

It means **layering many** controls, not one.

7. True

Physical access defeats firewalls and more.

8. True

Training is a rule/policy = managerial.

9. True

Long open times suggest an extra person slipped through.

10. residual

Residual risk remains after avoid/transfer/mitigate.