1. Encrypting data mainly protects which CIA goal?

   ☐ Availability

   ☐ Authority

   ☐ Integrity

   ☐ Confidentiality

2. Slipping through a secured door behind someone WITHOUT their knowledge is...

   ☐ card cloning

   ☐ tailgating

   ☐ piggybacking

   ☐ shoulder surfing

3. Investigators at Y-12 found that broken cameras and ignored alarms helped the intruders.

   ☐ True ☐ False

4. Where are cameras most useful?

   ☐ Facing a blank wall

   ☐ In empty storage closets

   ☐ Inside a locked safe

   ☐ At points of ingress and egress

5. A risk exists when a threat exploits a _____ to harm an asset.

   ☐ policy

   ☐ vulnerability

   ☐ backup

   ☐ firewall

6. A server with sensitive data in an unlocked, unmonitored room is what risk?

   ☐ Low

   ☐ Moderate

   ☐ High

   ☐ No risk

exercises.lol exercises.com.cn

   ☐ True ☐ False

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

   ☐ True ☐ False

9. Defense in depth means using a single very strong control.

   ☐ True ☐ False

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

    ☐ True ☐ False

1. **Confidentiality**

   Encryption hides data = **confidentiality**.

2. **tailgating**

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

3. **True**

   Controls must work and be acted on.

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. **High**

   Sensitive + no access control = **high** risk.

7. **True**

   Better than a shared key.

8. **True**

   Long open times suggest an extra person slipped through.

9. **False**

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

10. **True**

    Physical access defeats firewalls and more.

exercises.lol exercises.com.cn