AP CYBERSECURITY • EXERCISE SHEET

2.2 Physical Vulnerabilities and Attacks

Name: _____ Class: _____ Date: _____ **Total: 10 marks**

Objective

Build the skills to answer exam questions on **physical attacks** 物理攻击 and rating physical risk.

You must be able to:

- distinguish **piggybacking** 尾随（获许可）from **tailgating** 尾随（未察觉）
- describe shoulder surfing, dumpster diving, and card cloning
- rate physical risk as high, moderate, or low with a reason

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Piggybacking vs tailgating

Piggybacking tricks an authorised person into holding the door (with their cooperation). Tailgating slips in behind them without their knowledge. The difference is whether the victim is aware.

■ Rating physical risk

High = sensitive systems in a space with no controlled access. Moderate = an unimportant area that is a foothold to reach other resources. Low = a low-value asset unlikely to be attacked.

2 Practice

2.1 State the difference between **piggybacking** and **tailgating**. [2]

2.2 Describe **shoulder surfing**. [2]

2.3 A server with customer data sits in an unlocked room off an unmonitored hallway.

(a) State the risk level (high/moderate/low). [1]

(b) Justify your answer. [1]

3 Exam-style questions

3.1 Slipping through a secure door behind someone WITHOUT their knowledge is [1]

- **A** piggybacking
- **B** tailgating
- **C** shoulder surfing
- **D** card cloning

3.2 A locked warehouse of non-critical computers that could be a foothold to other systems is best rated as [1]

- **A** high risk
- **B** moderate risk
- **C** low risk
- **D** no risk

3.3 An attacker copies an employee's access card.

(a) Name this attack. [1]

(b) State one consequence of a successful attack. [1]

4 Go further

- work through the **2.2 Physical Vulnerabilities and Attacks** lesson on the **Learn** page;
- read the **Securing Spaces** section of the AP Cybersecurity handout on the **Know** page.

Solutions

2.1 piggybacking tricks an authorised person into helping/holding the door; tailgating slips in unnoticed without their knowledge.

2.2 watching a user as they enter a password or read sensitive information, sometimes recording it for later.

2.3 (a) high. (b) sensitive data with no controlled access makes it high-impact and easy to exploit.

3.1 B. tailgating is unnoticed; piggybacking is with consent.

3.2 B. a foothold to other resources is the classic moderate risk.

3.3 (a) card cloning. (b) the attacker can enter any area the employee is authorised for.