

Week 7

AP Cybersecurity

Homework bundle for this week

本周作业合集

exercises.lol

Contents 目录

Topic 2 quiz	2
Exercise sheet 2.1	5
Past-paper questions 2.1	8
Exercise sheet 2.2	10
Past-paper questions 2.2	14
Exercise sheet 2.3	15
Exercise sheet 2.4	18

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.

2.1 Cyber Foundations

Name: _____ Class: _____ Date: _____

Total: 13 marks

KEY WORDS risk 风险 • confidentiality 保密性 • detective 检测性 • physical 物理 • cia triad 中央情报三要素

Objective

Build the skills to answer exam questions on the **CIA triad** 中央情报三要素, **risk** 风险, and types of security control.

You must be able to:

- state the CIA triad and say which goal a control protects
- define risk and the four risk responses (avoid, transfer, mitigate, accept)
- classify controls by type (physical/technical/managerial) and function (preventative/detective/corrective)

1 Worked examples

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

■ The CIA triad

Confidentiality = only authorised people read the data. Integrity = the data is accurate and unaltered. Availability = it is there when needed. Encryption serves confidentiality, a hash checks integrity, a backup serves availability.

■ Classifying controls

By type: physical (locks, fences), technical (firewalls, encryption), managerial (policies). By function: preventative (a lock), detective (a camera), corrective (patching). A camera is physical by type and detective by function.

2 Practice

2.1 State the three goals of the **CIA triad**. [3]

2.2 Define **risk** in terms of a threat, a vulnerability, and an asset. [2]

2.3 Classify each control below.

- (a) A door lock - by function (preventative/detective/corrective)? [1]
- (b) A CCTV camera - by function? [1]
- (c) Patching a vulnerability - by function? [1]
-
-
-

3 Exam-style questions

3.1 Encrypting a stored file mainly protects which CIA goal? [1]

- **A** availability
 - **B** confidentiality
 - **C** integrity
 - **D** authority
-

3.2 An organisation buys insurance against a cyber loss. Which risk response is this? [1]

- **A** avoid
 - **B** transfer
 - **C** mitigate
 - **D** accept
-

3.3 A company adds a firewall, a camera, and a written access-review policy.

(a) Classify each by type (physical/technical/managerial). [3]

Solutions

2.1 confidentiality; integrity; availability.

2.2 risk occurs when a threat can exploit a vulnerability to compromise an asset.

2.3 (a) preventative. (b) detective. (c) corrective.

3.1 B. encryption hides data, protecting confidentiality.

3.2 B. shifting the burden to an insurer is transference.

3.3 (a) firewall = technical; camera = physical; access-review policy = managerial.

9. How does the email's claim that "Over 92% of employees have already completed the verification" attempt to pressure the recipient into responding to the email?
- (A) By framing the request as routine HR communication that seems safe, showing the use of familiarity
 - (B) By implying that the opportunity to comply is limited and may soon be lost, showing the use of scarcity
 - (C) By presenting the request as coming from those in power and intimidating the recipient, showing the use of authority
 - (D) By applying social pressure and making the recipient believe most coworkers have already acted, showing the use of consensus

16. A state's National Guard base is documenting cybersecurity risks from physical vulnerabilities. Which of the following would be classified as a moderate risk?
- (A) An unlocked trailer containing non-networked office equipment that cannot be used to access sensitive systems
 - (B) A locked warehouse with noncritical computers that could be a foothold to access other network resources
 - (C) A publicly accessible touchscreen directory for visitors that contains no sensitive data and is unlikely to be exploited
 - (D) A main server room that contains sensitive systems and information and does not have sufficiently restricted or controlled access

Questions 17 through 20 refer to the following.

Consider the following article.

Small Town Bank Disrupts Attempted Cyber Attack on Customer Database

Fairgrove Community Bank, a local financial institution serving residents of central Kentucky, reported that it successfully stopped a cyber intrusion attempt earlier this week aimed at its customer database.

The attack was detected on Tuesday afternoon when automated security systems flagged unusual database queries originating from the bank's online loan application form. Investigators determined that the form was being used to input malicious code.

"One of the strings the adversary submitted included ' OR '1'='1';--', " said James Holloway, a network administrator at Fairgrove Community Bank. "That's a common trick pulled from online tutorials."

Holloway said the attacker did not succeed in accessing any customer data, but the attempt revealed a flaw in the bank's web application.

Fairgrove Community Bank's security team has since patched the vulnerability. No data was compromised, and banking operations continued without interruption.

"This wasn't some advanced adversary," Holloway added. "They were copying code from the internet and testing to see if anything would work. But even simple attacks like this can work if we don't implement best practices."

Fairgrove Community Bank says it is conducting a full audit of its customer-facing applications to ensure proper protections are in place.

17. Which of the following best describes the adversary in this scenario?
- (A) Cyberterrorist
 - (B) Script kiddie
 - (C) State actor
 - (D) Insider

2.2 Physical Vulnerabilities and Attacks

Name: _____ Class: _____ Date: _____

Total: 10 marks

KEY WORDS piggybacking 尾随 • card cloning 门禁卡复制 • shoulder surfing 肩窥 • foothold 立足点
• dumpster diving 翻垃圾搜集情报

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]

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.

16. A state's National Guard base is documenting cybersecurity risks from physical vulnerabilities. Which of the following would be classified as a moderate risk?
- (A) An unlocked trailer containing non-networked office equipment that cannot be used to access sensitive systems
 - (B) A locked warehouse with noncritical computers that could be a foothold to access other network resources
 - (C) A publicly accessible touchscreen directory for visitors that contains no sensitive data and is unlikely to be exploited
 - (D) A main server room that contains sensitive systems and information and does not have sufficiently restricted or controlled access

Questions 17 through 20 refer to the following.

Consider the following article.

Small Town Bank Disrupts Attempted Cyber Attack on Customer Database

Fairgrove Community Bank, a local financial institution serving residents of central Kentucky, reported that it successfully stopped a cyber intrusion attempt earlier this week aimed at its customer database.

The attack was detected on Tuesday afternoon when automated security systems flagged unusual database queries originating from the bank's online loan application form. Investigators determined that the form was being used to input malicious code.

"One of the strings the adversary submitted included ' OR '1'='1';--', " said James Holloway, a network administrator at Fairgrove Community Bank. "That's a common trick pulled from online tutorials."

Holloway said the attacker did not succeed in accessing any customer data, but the attempt revealed a flaw in the bank's web application.

Fairgrove Community Bank's security team has since patched the vulnerability. No data was compromised, and banking operations continued without interruption.

"This wasn't some advanced adversary," Holloway added. "They were copying code from the internet and testing to see if anything would work. But even simple attacks like this can work if we don't implement best practices."

Fairgrove Community Bank says it is conducting a full audit of its customer-facing applications to ensure proper protections are in place.

2.3 Protecting Physical Spaces

Name: _____ Class: _____ Date: _____

Total: 11 marks

KEY WORDS access control vestibule 门禁前室 • ups 不间断电源 • card readers 读卡器 • bollards 防撞柱
• managerial 管理

Objective

Build the skills to answer exam questions on managerial and physical controls that protect a workspace.

You must be able to:

- give managerial controls: awareness training, workstation and clean-desk policies
- give physical controls: locks, bollards, card readers, an access control vestibule, a UPS 不间断电源
- explain how each control mitigates a specific physical attack

1 Worked examples

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

■ Managerial vs physical

Managerial controls are rules and training (a clean-desk policy, awareness training). Physical controls are objects that guard the space (locks, fences, bollards, card readers, an access control vestibule).

■ The access control vestibule

A two-door airlock: the first door must close before the second opens, so only one person passes at a time. This defeats piggybacking and tailgating by design.

2 Practice

2.1 State two managerial controls that protect a physical workspace. [2]

2.2 Explain how an **access control vestibule** stops piggybacking. [2]

2.3 State what a **UPS** does and why it matters.

[2]

3 Exam-style questions

3.1 Which of these is a managerial control?

[1]

- **A** a bollard
 - **B** a card reader
 - **C** a clean-desk policy
 - **D** a door lock
-

3.2 Disabling USB ports on office computers primarily prevents

[1]

- **A** power outages
 - **B** malware from external drives
 - **C** shoulder surfing
 - **D** network flooding
-

3.3 An office wants to stop unauthorised people entering a secure area.

(a) Name one physical control they could install.

[1]

(b) Explain how it mitigates the risk.

[2]

Solutions

2.1 any two of: security-awareness training; a workstation security policy; a clean-desk policy.

2.2 it is a two-door airlock letting one person pass at a time, so no one can follow an authorised person through.

2.3 a UPS provides backup power in an outage, keeping critical devices and services available.

3.1 C. a policy is a managerial (rule-based) control.

3.2 B. blocking USB drives stops malware being loaded from them.

3.3 (a) any of: a card reader / an access control vestibule / a lock. (b) e.g. a card reader denies entry to unauthorised badges and logs who enters and when.

2.4 Detecting Physical Attacks

Name: _____ Class: _____ Date: _____

Total: 10 marks

KEY WORDS motion sensors 运动传感器 • points of ingress and egress 出入口 • physical attacks 物理攻击
• physical 物理 • piggybacking 尾随 (获许可)

Objective

Build the skills to answer exam questions on detecting physical attacks and placing detection controls well.

You must be able to:

- list controls that detect physical attacks: cameras, guards, motion sensors
- explain why placement (entrances, low-traffic areas) matters
- read entry logs (door-open times) for signs of piggybacking

1 Worked examples

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

■ Placement matters

Cameras belong at points of ingress and egress. Motion sensors belong in low-traffic sensitive areas like server rooms - in a busy hallway they cause constant false alarms and get ignored.

■ Reading entry logs

A door that normally opens for 2 seconds but stayed open 15 seconds is a clue that someone piggybacked through behind an authorised employee.

2 Practice

2.1 State two controls that DETECT (rather than prevent) physical attacks. [2]

2.2 Explain why a motion sensor should not be placed in a busy hallway. [2]

2.3 An entry log shows a secure door was held open for 20 seconds, far longer than normal.

(a) State what this could indicate. [1]

(b) Explain your reasoning. [1]

3 Exam-style questions

3.1 Where are cameras MOST useful for detecting physical attacks? [1]

- **A** inside a locked safe
 - **B** at points of ingress and egress
 - **C** facing a blank wall
 - **D** in an empty closet
-

3.2 A stationary guard is best placed [1]

- **A** patrolling a large perimeter
 - **B** at a point that funnels traffic, like a main entrance
 - **C** in a distant unused room
 - **D** outside the property boundary
-

3.3 A company installs cameras and motion sensors.

(a) State one advantage of pairing cameras with motion sensors. [1]

(b) State the best placement for the motion sensors. [1]

Solutions

2.1 any two of: cameras; security guards; motion sensors.

2.2 constant movement causes many false alarms, so staff stop taking the alerts seriously.

2.3 (a) piggybacking / tailgating. (b) a door held open unusually long suggests an extra person passed through.

3.1 B. entrances and exits capture who comes and goes.

3.2 B. a fixed guard is effective where traffic is funnelled.

3.3 (a) when a sensor triggers, defenders can use the camera to verify a real breach. (b) in low-traffic sensitive areas such as server rooms.