

Securing Spaces

AP Cybersecurity ■ Unit 2

AP Cybersecurity



Securing Spaces

What we will cover

- 1 The CIA triad
- 2 Adversaries & attack phases
- 3 Risk & how to manage it
- 4 Classifying controls
- 5 Physical attacks
- 6 Protecting & detecting

1 Foundations

The CIA triad – the three goals of security

Every control protects at least one part of the **CIA triad** 信息安全三要素:

- **Confidentiality** 保密性 – only authorised people can read it
- **Integrity** 完整性 – it is accurate and unaltered
- **Availability** 可用性 – it is there when needed

Be ready to say which goal a control serves: encryption → confidentiality; a hash → integrity; a backup → availability.

Who attacks, and why

Script kiddie 脚本小子
reuses others' tools –
greed or recognition

Hactivist 黑客活动分子
a political, social
or personal cause

Insider 内部人员
already has legitimate access

Cyberterrorist 网络恐怖分子
disrupts critical infrastructure

Transnational criminal organisations 跨国犯罪组织 chase money – ransomware and stolen data.

Attacks unfold in phases

reconnaissance 侦察 –
often **OSINT** 公开来源情报

initial access,
then persistence

**lateral move-
ment** 横向移动

act on the goal,
evade detection



Padlock physical

Risk – and the four ways to manage it

A **risk** 风险 appears when a **threat** 威胁 can exploit a **vulnerability** 漏洞 to compromise an **asset** 资产.

Assess it by weighing **likelihood** 可能性 against **severity** 严重性.

You accept the leftover **residual risk** 剩余风险 because perfect security is impossible.

Avoid 规避
stop the activity

Transfer 转移
e.g. an insurer

Mitigate 缓解
add controls

Accept 接受
live with it

Classifying a control – two ways, always

By type

physical 物理 – locks, fences, guards
technical 技术 – firewalls, encryption
managerial 管理 – policies and procedures

By function

preventative 预防性
– stop it (a lock)
detective 检测性
– spot it (a camera)
corrective 纠正性 – fix it (patching)

Exam answers name **both**: a door lock is **physical** by type and **preventative** by function.

Worked example – rate the risk, classify the fix

A hospital stores patient records on an unencrypted server in an unlocked room

The asset is highly sensitive (patient data, protected by law) and the vulnerability is easy to exploit (no encryption, no access control).

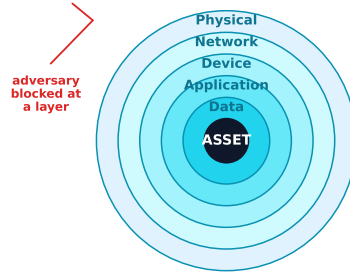
⇒ HIGH risk

The fix – a door lock – is **physical** by type and **preventative** by function.

High risk needs BOTH high value and easy exploitation. A “foothold to other systems” is the classic moderate risk.

Defence in depth

The best strategy layers many controls – **defence in depth** 纵深防御. If an adversary bypasses one layer, another still stands. Layers: human, physical, network, device, application, data.



one breach does not expose the asset

This is the model answer whenever a question asks why one control is not enough.

2 Physical attacks

Physical attacks – walking straight in

Digital security means nothing if an adversary can simply walk in. Most **physical attacks** 物理攻击 begin with social engineering:

Piggybacking 尾随（获许可）
the authorised person
holds the door – tricked

Tailgating 尾随（未察觉）
slipping through unnoticed

Shoulder surfing 肩窥
watching you type

Dumpster diving 翻垃圾搜集情报
card cloning 门禁卡复制

Piggybacking has consent (you were tricked); tailgating does not (you never knew). The exam tests this exact pair.

Protecting physical spaces

Managerial first: security-awareness training (do not badge strangers in) and a workstation policy – locking devices, a **clean desk policy** 清桌政策, privacy screens.

With physical access an adversary can cut power, copy data, or plug in a **key-logger** 键盘记录器.

fences, gates, **bol-lards** 防撞柱 – deter

card readers 读卡器
– log and restrict

access control vestibule 门禁前室
– stops piggybacking

disabled USB ports;
a **UPS** 不间断电源

Detecting physical attacks – placement matters

Some controls **detect** rather than prevent: cameras record, guards respond, **motion sensors** 运动传感器 alert – and employees often notice an intruder first.

Cameras belong at **points of ingress and egress** 出入口.

Motion sensors work in **low-traffic** areas like server rooms. Put one in a busy hallway and the **constant false alarms** make everyone ignore them.

A stationary guard protects a fixed high-value point; a **patrolling guard** is harder to plan around. Reviewing **door-open times** can reveal piggybacking – a door held open too long is suspicious.

3

Recap

Unit 2 – key takeaways

1 CIA

say WHICH goal a control serves
– C, I or A

2 Risk

threat × vulnerability on an asset;
avoid, transfer, mitigate, accept

3 Classify twice

by type
(physical/technical/managerial)
AND function

4 Depth

layers – the answer to “why is one
control not enough?”

Check yourself

- 1 Which CIA goal does a hash protect?
- 2 Piggybacking or tailgating: the victim knows they let you in?
- 3 Classify a security camera by type and by function.
- 4 Name the four ways to manage a risk.

Answers 1. integrity 2. piggybacking 3. physical; detective 4. avoid, transfer, mitigate, accept