

AP Cybersecurity | Unit 2

2.1 Assets, Spaces, and Exposure

Solutions

Reference scenario

Inventory a classroom with shared tablets, an unlocked cabinet, and a visitor-accessible network socket.

Asset: 12 tablets

Storage: unlocked cabinet

Port: visitor-accessible

Inventory: last checked 6 months ago

2.1.1

Identify two assets and two exposures in a reception area with a shared computer and printed visitor records.

Assets include the computer and personal information on the paper records. Exposures include unattended unlocked access and records visible or removable by visitors.

2.1.2

Why should an asset inventory record an owner and location rather than only a device serial number?

Ownership assigns responsibility and location supports verification and incident response. A serial number identifies the asset but does not explain who should control it or where it should be.

AP Cybersecurity | Unit 2

2.2 Preventive Physical Controls

Solutions

Reference scenario

Choose preventive controls for an equipment room while keeping emergency procedures usable.

Door: routinely propped open

Visitor entry: unescorted

Equipment checkout: undocumented

2.2.1

Compare a locked cabinet and a camera as controls for spare laptops.

A locked cabinet restricts access before removal. A camera supports deterrence and investigation but may not physically prevent removal. The two serve different functions and can complement each other.

2.2.2

Name one verification test after introducing badge-based equipment-room entry.

Confirm an authorized badge admits its holder, an unauthorized badge is denied, and the access event is logged. Also verify the approved emergency-access process.

AP Cybersecurity | Unit 2

2.3 Detection and Accountability

Solutions

Reference scenario

Correlate records after a tablet is reported missing.

14:02 door event: staff badge accepted

14:05 tablet checkout: no entry

14:30 inventory: one tablet absent

2.3.1

What can a door log prove more directly: that a badge was accepted, or that the named person personally entered?

It directly records acceptance of a credential. Identity of the actual person may require corroboration because badges can be shared, lost, or misused.

2.3.2

Why are synchronized timestamps useful when comparing door, device, and camera records?

They help establish event order and correlate activity. If clocks differ, document and account for the offsets rather than creating a false timeline.

AP Cybersecurity | Unit 2

2.4 Tailgating, Shoulder Surfing, and Device Handling

Solutions

Reference scenario

A visitor follows a student into a restricted lab and uses an unlocked workstation.

Entry: no separate credential

Workstation: signed-in session

Visitor escort: absent

2.4.1

What behavior reduces shoulder-surfing risk at a public kiosk?

Protect the view of sensitive entry, avoid displaying unnecessary personal information, and use an appropriate privacy screen or placement. Screen locking protects the session when the user leaves.

2.4.2

Write three rules for handing a shared tablet from one user to another.

Sign out of the previous session, verify the next user through the approved checkout process, and record the handoff. Apply screen-lock and storage rules when it is not in active use.