

AP Cybersecurity | Unit 1

1.1 Security Thinking and Risk Language

Solutions

Reference scenario

A scheduling account has a reused password and can export all student records. Identify the risk chain.

Asset: student records

Condition: reused password and broad export access

Observed compromise: not established

1.1.1

A former employee still has an active account. Identify the vulnerability and a plausible threat.

The vulnerability is access that was not removed after the role ended. A plausible threat is use of that account to read or alter organizational data without authorization.

1.1.2

Compare MFA and least privilege for this account. Which part of the risk does each reduce?

MFA reduces some forms of credential-only account takeover. Least privilege limits which data or actions the account can reach if it is misused. Neither alone guarantees the account cannot be abused.

AP Cybersecurity | Unit 1

1.2 Social Engineering and Human Workflow

Solutions

Reference scenario

A message claims to be the principal and demands an urgent payment-code screenshot. Choose a trusted response.

Pressure: immediate action

Requested secret: payment verification code

Contact method: unfamiliar message account

1.2.1

Why does a familiar display name not establish that a message came from a trusted staff member?

Display names can be copied or forged. Verify unusual requests through a separately established contact method and inspect relevant message evidence.

1.2.2

Propose a workflow control stronger than a reminder to be careful for urgent payment requests.

Require independent confirmation and a second authorized approval before payment changes or transfers. Document exceptions and give staff a clear reporting path.

AP Cybersecurity | Unit 1

1.3 Authentication and Account Protection

Solutions

Reference scenario

A teacher logs in successfully but cannot edit payroll records. Separate two access decisions.

Identity check: successful

Role: teacher

Payroll edit permission: absent

1.3.1

Are a password and a PIN necessarily two distinct authentication factors? Explain.

Not necessarily. Both are knowledge factors. Multifactor authentication requires different factor categories, such as knowledge plus possession.

1.3.2

A temporary administrator changes roles. What account lifecycle action should follow?

Remove unnecessary elevated permissions promptly, retain an individual identity for accountability, and verify that the new role retains only the access its work requires.

AP Cybersecurity | Unit 1

1.4 Adversaries, Motives, and AI-Enabled Risk

Solutions

Reference scenario

A contractor account downloads an unusually large set of files after its engagement ends. Distinguish evidence from motive.

Account: former-contractor
Transfer: 2 GB
Time: outside scheduled work
Role end date: previous week

1.4.1

An AI assistant confidently calls one failed login an insider attack. Why is that conclusion unsupported?

A failed login can arise from an ordinary typo, an automated attempt, or several other causes. One event does not establish actor identity or intent; correlate additional evidence.

1.4.2

What data-handling precaution applies before using an external AI tool to summarize incident records?

Use an approved tool and share only the permitted minimum. Remove secrets and unnecessary personal or confidential data, then verify the summary against the original records.