Hospital Ransomware

Industry: Healthcare
Observed Symptoms
• Doctors cannot access patient records.
• Surgeries are delayed.
• Ambulances are diverted.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Availability

Hospital Ransomware — Instructor Side

Answer Key

Likely Vulnerability
Employee clicked a phishing email carrying ransomware.

Diagnostic Clues
Files renamed, ransom note, massive file access from one account.

Recommended Defenses
Email filtering, MFA, user training, offline backups.

Mnemonic
TVER: Threat → Vulnerability → Exploit → Risk

Bonus Challenge
Which part failed first: People, Process, or Technology?

Airline Reservation System

Industry: Transportation
Observed Symptoms
• Reservation system unavailable.
• Thousands of flights delayed.
• Passengers stranded.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Availability

Airline Reservation System — Instructor Side

Answer Key

Likely Vulnerability
Administrator reused a breached password.

Diagnostic Clues
Overseas login, new admin account.

Recommended Defenses
Unique passwords, MFA, login alerts.

Mnemonic
TVER: Threat → Vulnerability → Exploit → Risk

Bonus Challenge
Which part failed first: People, Process, or Technology?

Personal Savings Account

Industry: Finance
Observed Symptoms
• Savings account emptied.
• Fraudulent transfers detected.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Confidentiality

Personal Savings Account — Instructor Side

Answer Key

Likely Vulnerability
Victim entered credentials on fake banking site.

Diagnostic Clues
Unknown login location, password reset, transfers.

Recommended Defenses
MFA, password manager, verify URLs.

Mnemonic
TVER: Threat → Vulnerability → Exploit → Risk

Bonus Challenge
Which part failed first: People, Process, or Technology?

High School Grades

Industry: Education
Observed Symptoms
• Grades unexpectedly changed.
• Students dispute records.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Integrity

High School Grades — Instructor Side

Answer Key

Likely Vulnerability
Teacher password exposed on sticky note.

Diagnostic Clues
After-hours logins from classroom.

Recommended Defenses
Password hygiene, auto-lock screens.

Mnemonic
TVER: Threat → Vulnerability → Exploit → Risk

Bonus Challenge
Which part failed first: People, Process, or Technology?

Water Treatment Plant

Industry: Critical Infrastructure
Observed Symptoms
• Chemical settings changed.
• Public safety concern.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Integrity

Water Treatment Plant — Instructor Side

Answer Key

Likely Vulnerability
Weak remote access credentials.

Diagnostic Clues
Remote login followed by configuration change.

Recommended Defenses
VPN, MFA, least privilege.

Mnemonic
TVER: Threat → Vulnerability → Exploit → Risk

Bonus Challenge
Which part failed first: People, Process, or Technology?

Online Store

Industry: Retail
Observed Symptoms
• Customer card data stolen.
• Business reputation damaged.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Confidentiality

Online Store — Instructor Side

Answer Key

Likely Vulnerability
Unpatched web server exploited.

Diagnostic Clues
Exploit requests in logs, DB exfiltration.

Recommended Defenses
Patching, WAF.

Mnemonic
TVER: Threat → Vulnerability → Exploit → Risk

Bonus Challenge
Which part failed first: People, Process, or Technology?

Smart Home

Industry: Consumer IoT
Observed Symptoms
• Security cameras viewed remotely.
• Family privacy lost.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Confidentiality

Smart Home — Instructor Side

Answer Key

Likely Vulnerability
Default password never changed.

Diagnostic Clues
Unknown devices and overseas logins.

Recommended Defenses
Change defaults, firmware updates.

Mnemonic
TVER: Threat → Vulnerability → Exploit → Risk

Bonus Challenge
Which part failed first: People, Process, or Technology?

Factory Shutdown

Industry: Manufacturing
Observed Symptoms
• Production halted.
• Missed customer deliveries.

Your Team's Mission
1. What asset is being protected?
2. Which CIA property is most affected?
3. What vulnerability might exist?
4. What evidence/logs would you examine?
5. How would you prevent this attack?
Difficulty: ★■■ **CIA Focus:** Availability

Factory Shutdown — Instructor Side

Answer Key

Likely Vulnerability
Malware from infected USB drive.

Diagnostic Clues
Malware immediately after USB insertion.

Recommended Defenses
USB controls, endpoint security.

Mnemonic
TVER: Threat → Vulnerability → Exploit → Risk

Bonus Challenge
Which part failed first: People, Process, or Technology?