Unit 2: Securing Spaces

Content Area: **Business**
Course(s): **Generic Course**
Time Period: **Semester 1**
Length: **5 weeks**
Status: **Published**

Standards

8.1.12.CS.2	Model interactions between application software, system software, and hardware.
8.1.12.NI.2	Evaluate security measures to address various common security threats.
8.1.12.NI.3	Explain how the needs of users and the sensitivity of data determine the level of security implemented.
8.1.12.NI.4	Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
8.2.12.ED.1	Use research to design and create a product or system that addresses a problem and make modifications based on input from potential consumers.
8.2.12.ED.5	Evaluate the effectiveness of a product or system based on factors that are related to its requirements, specifications, and constraints (e.g., safety, reliability, economic considerations, quality control, environmental concerns, manufacturability, maintenance and repair, ergonomics).

Enduring Understandings

EU 2.1: Structured Risk and Layered Defense
Total security is an illusion, so defenders must prioritize assets and slow down attackers using multiple, distinct layers of defense. By mapping out an adversary's motivation and tracking their step-by-step attack phases, organizations can choose whether to avoid, accept, mitigate, or transfer risks, ensuring that if one control fails, another is waiting behind it.

EU 2.2: The Digital Risk of Physical Flaws
A system with perfect digital encryption is still entirely vulnerable if an attacker can physically touch the hardware. Physical proximity allows low-tech exploits (like looking over someone's shoulder) and high-tech hardware tampering (like plugging in a hidden keylogger) to completely undermine digital access controls and compromise data.

EU 2.3: Proactive Prevention of Physical Spaces
Securing a physical facility requires a blend of clear workplace policies and strong structural barriers. To effectively prevent unauthorized entry, an organization must complement physical infrastructure (like fences, gates, and secure entryways) with managerial policies that train employees to recognize vulnerabilities and secure their workstations.

EU 2.4: Active Monitoring and Human Vigilance
Detection mechanisms are only effective if they provide accurate, timely alerts that human defenders can realistically act upon. While automated tools like cameras and motion sensors provide continuous surveillance,

informed employees are often the fastest line of defense for spotting anomalies, and sensor placement must be carefully tuned to prevent the alert fatigue caused by false alarms.

Essential Questions

Topic 2.1: Cyber Foundations

How do organizations use risk management strategies and defense-in-depth frameworks to classify adversaries, trace attack phases, and deploy overlapping layers of security controls?

Topic 2.2: Physical Vulnerabilities and Attacks

How do physical security breaches (such as tailgating, dumpster diving, or port manipulation) bypass digital protections to compromise the CIA triad?

Topic 2.3: Protecting Physical Spaces

How do security professionals layer managerial and physical controls (like bollards, vestibles, and policies) to ensure that a single physical breach does not expose an entire network?

Topic 2.4: Detecting Physical Attacks

How do organizations strategically place detection tools (like cameras, sensors, and guards) to catch physical intruders early while minimizing false alarms that disrupt operations?

Knowledge and Skills

Topic 2.1: Cyber Foundations

- Identify all eight social engineering tactics and the psychological principle behind each (2.1.A)
- Classify the five adversary types by skill level, motivation, and behavior (2.1.B)
- Identify and sequence all six phases of a cyberattack and match defenses to each phase (2.1.C)
- Describe the risk assessment process and produce a qualitative or quantitative risk rating (2.1.D)
- Apply all four risk management strategies and explain residual risk (2.1.E)
- Classify security controls by CIA principle, type (Physical/Technical/Managerial), and function (Preventive/Detective/Corrective) (2.1.F)
- Explain why defense-in-depth is necessary and describe how layers interact (2.1.G)

Topic 2.2: Physical Vulnerabilities and Attacks

- Identify and precisely distinguish piggybacking, tailgating, shoulder surfing, dumpster diving, and card cloning (2.2.A)
- Explain how threats exploit physical vulnerabilities through power disruption, port access, and keylogger installation (2.2.B)
- Assess and document physical risks using the high/moderate/low classification framework with CED criteria (2.2.C)
- Map each physical attack type to the CIA property or properties it violates
- Select the most effective physical control for each attack vector and explain why it directly addresses the mechanism

Topic 2.3: Protecting Physical Spaces

- Identify and describe managerial controls for physical security: security awareness training requirements and workstation security policy elements (2.3.A)
- Determine appropriate physical mitigation strategies for each identified risk: fencing, gates, bollards, locks, card readers, access control vestibules, USB port disabling, UPS systems (2.3.B)
- Apply defense-in-depth principles to physical space protection — layering controls so that bypassing one does not expose all assets
- Prioritize mitigations based on severity of risk and cost-effectiveness of the control
- Match the correct control type and function to each physical attack vector identified in Topic 2.2

Topic 2.4: Detecting Physical Attacks

- Identify cameras, security guards, motion sensors, locks, and access control vestibules as physical security detection controls (2.4.A)
- Determine effective placement of cameras, motion sensors, guards, and locks for detecting physical attacks (2.4.B)
- Apply detection techniques — cameras with facial recognition, motion detectors paired with cameras, and door-duration entry log analysis — to identify physical attacks (2.4.C)
- Recognize that employees working in a physical space are often the first to detect unauthorized persons (2.4.A.4)
- Explain why false alarms undermine detection effectiveness and how placement decisions prevent them (2.4.B.2)

Transfer Goals

Students will be able to analyze any environment to identify who the likely threats are, evaluate the risks, and plan a multi-layered defense to protect valuable assets.

Students will be able to recognize and secure everyday physical vulnerabilities, ensuring they do not allow

unauthorized people to follow them into secure areas, handle sensitive trash, or touch secure hardware.

Students will be able to select and combine different types of security tools—such as policies, electronic locks, and structural barriers—so that a failure in one area does not collapse the whole system.

Students will be able to strategically spot and set up monitoring tools to catch security breaches early while actively avoiding false alarms that cause people to ignore warnings.

Resources

AP Cybersecurity Course and Exam Description, Effective Fall 2026, College Board

AP Cybersecurity Course Framework, Effective 2026-2027 School Year, College Board

AP Cybersecurity Curriculum, by APCSExamPrep.com

Cybersecurity Curriculum Materials, by Cyber.org

Cyber Range, provided by Cyber.org