UNIT 9: Physical Controls

Estimated Time in Hours: 5

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
4 Data Security 1 Ethics	1.2, 4.2	- Classify controls as preventative, detective, or corrective and determine cost based on the type of control. - Create a physical control plan for a structure using estimated costs and requirements for use.

Guiding Questions:

- What are the three types of physical controls?
- Which type of physical control is more important? Most expensive?
- Can something that is a preventative control also be a corrective control?
- What is the difference between tailgating and piggybacking?
- What does defense in depth mean in the context of physical controls?
- How are redundant systems used?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
4.2.2 LO: Students will identify physical controls that are used to secure data.	• Computer, lecture slides, projector, graphic organizers, access to Internet • "Why No One Can Break Into The Most Secure Place In The World." *YouTube*, uploaded by The Infographics Show, 31 Aug 2019, https://youtu.be/XIMd2tMOD5g	• Review the three types of access control and how their purpose is to protect assets. • Explain how facilities must maintain physical protection to ensure other types of protection. Use Fort Knox in KY as an example of a place that relies heavily on physical controls. Throughout the unit you can put the student in the shoes of head of security at Fort Knox and tie all standards to the theme. • Use a video to highlight common physical controls. Consider accompanying with a viewing guide.

	(WARNING: only show first half of the video; it looks at physical controls from the perspective of an adversary and references graphic violence in the second half of the video)	
4.2.2a EK: Physical security controls are means and devices to control physical access to sensitive information and to protect the availability of the information.		• Categorize physical controls by preventative, detective, or corrective. Compare and contrast them. Emphasize how they must all be present in order to achieve physical controls. • Provide students with types of controls to classify as preventative, detective, or corrective.
4.2.2c EK: Commonly used physical controls include: limited entry points, redundant systems, and surveillance cameras.	• "InfoSec Video - Tailgating." *YouTube*, uploaded by Steven Burrell, 29 Oct 2016, https://www.youtube.com/watch?v=1fmLds7EZXs&feature=emb_logo	• Provide examples and pictures of preventative detective, and corrective controls. • Provide examples of how adversaries can circumvent security through tailgating and piggybacking. Elaborate how the controls can put a stop to these attacks. • Multi-factor authentication may be introduced here. Provide examples and ask students to categories the types of multi-factor. • Ask students how a person can use multi-factor to prove who they are before entering Fort Knox.

		• Emphasize the criticality of redundant systems in cybersecurity and security. Ask what would happen in the scenarios of disasters or sickness.
4.2.2b EK: Physical security is an important part of defense in depth. To provide comprehensive physical security, multiple systems and process must work together, like perimeter security, access control, and process management.		• Show how defense in depth is achieved through use of security zones, perimeter security, and specific controls. • Show examples of various security zones. • Ask students what addition layer of defense they could add to Fort Knox. • Ask students if there are any drawbacks to these layers of defense.
1.2 EU: Ethical reflection and judgement are required in considering the potential harms, benefits, and trade-offs involved in cybersecurity.		• Students should weigh the cost of different physical controls and determine whether an investment is efficient, ethical, and the good use of funds. • Activity: students should design a physical control plan for a generic structure (e.g., bank, school, government building) and include a cost breakdown for the controls.
8.1.1h EK: Cybersecurity events have led to the development of various cybersecurity career paths and various needs in order to prepare people for these new types of jobs.		• Explore a relevant career, such as cyber defense infrastructure support specialist.