UNIT 25: Design Trade-offs

Estimated Time in Hours: 5

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 1 Ethics 6 Adversarial Thinking 8 Implications	2.4	- Capstone Project.

Guiding Questions:

- What is the only safe assumption you can make about a system?
- Cybersecurity requires time, money, and expertise. Why all three?
- How does cybersecurity impact the technology on a system, and vice-versa?
- What can you do to prevent a "weakest link failure" in cybersecurity?
- Why should the environment be considered in cybersecurity?
- What are the responsibilities of a systems security analyst?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
2.4.1b EK: Key assumptions of systems are things such as whether only valid users are in the system, whether hardware is trusted, whether the software really does what it claims to do. 2.4.1a EK: An assumption in this context is an assertion about the security of a system being designed; it can be a valid or invalid assertion.		• As the students have learned, users often make assumptions about systems. They tend to trust entities with the personal information. Ask students if users can always trust systems. Ask them to list reasons why or why not. • Cybersecurity experts should question assumptions about systems. This process of checking, testing, and researching helps make a system more secure. Why? Because incorrect assumptions can lead to system failures. • In fact, the only assumption you can safely make about a system is that it is not safe. Confronting incorrect

2.4 EU: Identifying and questioning assumptions is a key part of making a system more secure. 2.4.1c EK: Incorrect assumptions lead to system failures. 2.4.1e EK: The only assumption you can safely make is that data and networks are not safe. 2.4.1d EK: When confronting incorrect assumptions, facing up to cyber attacks is an ongoing, and constantly evolving challenge.		assumptions and facing a cyber attack is an ongoing, constantly evolving task.
1.2.1c EK: Cybersecurity requires resources, including time, money, and expertise that also affects technological affordances. 6.1.3 LO: Students will understand how different system components impact the cybersecurity of a system design. 6.1.3a EK: Security is only as strong as the weakest link and is not limited to human actors.		• Let's review some things we have learned about cybersecurity. 1. It requires time, money, and expertise. 2. It impacts the technology that is placed in a system. 3. It is impacted by the different system components on a system. 4. It is only as strong as the weakest link (and this weak link could be single point of failure in a system and not a human). 5. It is impacted by humans as producers of system failure and humans as defenders against system failure. 6. It is impacted by change, as change introduces new ways for a system to fail. 7. It is impacted by the Internet and IoT devices, which create new vulnerabilities an adversary can exploit. 8. It can be negatively impacted by natural disasters and unintentional errors as well as adversaries.

6.1.3b EK: Human operators have dual roles: as producers and defenders against failure. 6.1.3d EK: Change introduces new forms of failure. 8.1.2f EK: The Internet and IoT devices create new vulnerabilities an adversary can exploit. 6.1.3c EK: Events ranging from natural disasters to unintentional errors can result in cybersecurity failures.		
6.1.3c EK: Events ranging from natural disasters to unintentional errors can result in cybersecurity failures.		• For a final project, students will play the role of a systems analyst. Explain that a systems security analyst conducts vulnerability scans and recognizes vulnerabilities in security systems then applies cybersecurity and privacy principles to organizational requirements. **Project Scenario**: A new business is opening in town, and the student(s) have been asked to help design the system. It is recommended that students model their designs on a small business they are already familiar with to make it easier. **Project Task**: The groups should design a secure network that includes a network topology and list of devices. They should also include a list of technical, administrative, and physical

		controls. The student(s) should pass the design to another student/team, to review. This review should include possible weaknesses in the design and suggested revisions.