Detailed Unit Descriptions

UNIT 1: WHAT IS CYBERSECURITY

Estimated Time in Hours: 5

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
7 Risk 1 Ethics 8 Implications	7.1	- Examine attack surface of a car. - Create a timeline of major cybersecurity-related events.

Guiding Questions:

- What is cybersecurity?
- What is the difference between threats, vulnerabilities, and attacks?
- How does one identify and prioritize the protection of information assets?
- What is a threat model, and how do you evaluate the trade-offs associated with defending against different threat sources?
- How do ethical obligations to society coexist with ethical obligations to one's family, friends, employer, local community, and even oneself?
- What is the progression of technology, and how did it lead to the development of cybersecurity needs and career paths?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
7.1.1 LO: Students will be able to differentiate between threats, vulnerabilities, and attacks. 7.1.1aEK: A vulnerability is a weakness or gap in a security program that can be exploited by	• Computer, lecture slides, projector, graphic organizers	• Using a car as an example, have students identify a way someone could attack a vehicle

threats to gain unauthorized access to an asset.		
7.1.1bEK: A threat is anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. 7.1.3a EK: Threats originate from internal (insider) and external sources such as nation states, multinational criminal organizations, and hacktivists/terrorists. 7.1.1 LO: Students will be able to differentiate between threats, vulnerabilities, and attacks.		• Provide the definition of threat and ask students to provide examples of threats.
7.1.3a EK: Threats originate from internal (insider) and external sources such as nation states, multinational criminal organizations, and hacktivists/terrorists. 7.1.3b EK: Bad actors in cyberspace are characterized by their resources,		• Provide examples of the major categories of threats (insider, nation state, criminal organization, hacktivists, and script kiddies). Have students compare and contrast these types in relation to resources, capabilities, techniques, motivations, and aversion to risk.

capabilities/techniques, motivations, and aversion to risk.		
7.1.1c EK: Attacks arise when threats exploit vulnerabilities. 7.1.1 LO: Students will be able to differentiate between threats, vulnerabilities, and attacks. 7.1.3b EK: Bad actors in cyberspace are characterized by their resources, capabilities/techniques, motivations, and aversion to risk.		• Using the car example, have students list threats, vulnerabilities, and attacks on a car. • Discuss possible attacker motivations. • Next list ways to mitigate these threats.
7.1.2a EK: Information assets must be identified. 7.1.2 LO: Students will be able to identify and prioritize the protection of information assets. 7.1.2b EK: Information assets are characterized and prioritized according to their need to be kept confidential, unchanged, and/or available, and their criticality/sensitivity.		• Using the car as an example, have students prioritize which assets are more important to the system. For example, an engine should get a higher priority than the radio, since the engine is needed to move the car. • Introduce the idea of the risk management framework.

7.1.2c EK: Risks to information assets are a function of the likelihood that a threat source will exploit a vulnerability, and the resulting damage if the attack is successful.		
7.1.3c EK: There are risks and solutions associated with closed/proprietary systems.		• Have students compare/contrast representative proprietary systems with their open source equivalents. Have students research risks associated with these systems.
8.1.1b EK: As technology progressed so did the use of both disinformation and information security in national, societal, and personal gain, often at the expense of another party.	• Internet	• Have students create a timeline of important cybersecurity events.
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.	• "NICE Cybersecurity Workforce Framework Work Roles." *NICCS*, https://niccs.us-cert.gov/nice-cybersecurity-workforce-framework-work-roles	• Introduce cybersecurity workforce roles.
1.3.2a EK: Ethical obligations are covenants that define a moral course of action and draw a line between right and wrong.	• Awad, Dsouza, Chang, and Tang. *Moral Machine.* The MIT Media Lab at the Massachusetts Institute of Technology,	• Define ethics. Possibly use the moral machine to guide students into seeing how ethics can have an impact on computer programming.

1.3.2 LO: Students will discuss how ethical obligations to society always coexist with ethical obligations to one's family, friends, employer, local community, and even oneself. 1.3.2b EK: Social responsibility is an ethical theory, in which individuals are accountable for fulfilling their civic duty; the actions of an individual must benefit the whole of society.	http://moralmachine.mit.edu/ • The Computer Ethics Institute. "The Ten Commandments of Computer Ethics." The Computer Professionals for Social Responsibility, *CPSR.org,* http://cpsr.org/issues/ethics/cei/	• Using the 10 Commandments of Computer Ethics by the Computer Ethics Institute, discuss each one. • Have students put these 10 commandments in context of their families, friends, employers, communities, and society. • Discuss the definition of social responsibility and provide examples (use graphic organizer here). Examples: philanthropic, ethical, legal, and economic.