Hairston_Williams | Planning & Pacing Guide

Contents

Course Planning and Pacing by Unit

Unit 1: What is Cybersecurity – Big Ideas 7, 1, 8
Unit 2: CIA Triad – Big Ideas 2, 1, 6, 5
Unit 3: What Is Hardware and How Do Computers Work – Big Ideas 5, 8
Unit 4: Cybersecurity Is Global – Big Ideas 8,1
Unit 5: Cyber Law – Big Ideas 4, 1, 8
Unit 6: Data Security Concerns – Big Ideas 4, 1, 8
Unit 7: Principles of Software Design (Overview) – Big Idea 2
Unit 8: Cybersecurity Business Economics – Big Ideas 8, 1
Unit 9: Physical Controls – Big Ideas 4, 1
Unit 10: Cryptography – Big Ideas 4, 8
Unit 11: Authentication & Identity Management – Big Ideas 4, 6, 2
Unit 12: Why Is Software Vulnerable – Big Ideas 7, 1, 2, 8
Unit 13: Software Vulnerabilities – Big Ideas 5, 1, 2
Unit 14: OSI Model – Big Ideas 3, 2

Unit 15: Network Standards & Protocols – Big Ideas 3, 2
Unit 16: Complexity of Cyber Space – Big Ideas 7, 6
Unit 17: Why Is the Internet Vulnerable – Big Ideas 3, 1
Unit 18: Cyber Attack Chain – Big Ideas 7, 6, 8
Unit 19: Network Security Technologies – Big Ideas 3, 6, 2
Unit 20: Network Meets Cryptography – Big Ideas 7, 2
Unit 21: Hardware & Software Integration – Big Ideas 5, 2
Unit 22: Common Hardware Vulnerabilities – Big Ideas 5, 7, 2
Unit 23: Conducting Security Testing & Assessments – Big Ideas 7, 1, 6
Unit 24: Cyber Physical Systems – Big Ideas 5, 4, 2, 8
Unit 25: Design Trade-offs – Big Ideas 2, 1, 6, 8

Instructional Setting

School	This course is designed specifically for students who are Deaf and hard-of-hearing. It will be implemented in schools for the Deaf, where the average class size is fewer than 10 students. It will be an elective course, taught by a trained teacher.
Student Population	• Percentage of students receiving free or reduced-price lunches will vary school to school. • As the curriculum is for students who are Deaf and hard-of-hearing, many will consider English as a second language. Their primary language is ASL. • The percentage of college-bound students is unknown, as it varies from institution to institution.
Instructional Time	The course is designed to be taught with traditional scheduling; however, it may be adapted for other bell schedules. A Windows computer lab is suggested.
Student Preparation	As this is an introductory course, no prerequisites are required. It is intended for 9th grade students.
Primary Planning Resources	Resources are listed in the materials section of each unit.

Overview of the Course

Course Goals

This course is designed to provide fundamental knowledge in the field of cybersecurity. It begins with defining cybersecurity and its need at the individual, corporate, government, and international levels. Next, it discusses the CIA triad and gives a basic introduction to computer hardware, which are knowledge units needed for the rest of the course. After providing this foundational introduction to the field, the course explores how cybersecurity is integrated into the fabric of human life by understanding its impact on nations, laws, economics, and personal data. The course then becomes more technical in nature, introducing students to the principles of software design, physical security controls, cryptography, authentication and identity management, software vulnerabilities, the OSI model, network standards and protocols, the Internet, and hardware and software integration. The course ends by teaching security testing and assessment, securing cyber physical systems, and design trade-offs.

Throughout the course, ethics, think like an adversary, careers, and historic components are incorporated to provide students with consistent instruction of ideas necessary to build the next generation of cybersecurity experts.

Major Projects & Performance Tasks

Major projects include designing a computer, setting up virtual machines, securing various operations systems in virtual machine environments, designing a secure network environment, and securing a cyber physical system.

At the completion of the course, students will have the foundational knowledge to prepare them for study in the fields of cybersecurity computer engineering, computer science, information systems, or related areas.

Cybersecurity Curriculum Guidelines Mapping

Unit Number	Big Idea	Enduring Understanding	Learning Objective	Essential Knowledge Statement
1: What is Cyber-security	7 Risk, 1 Ethics, 8 Implications	7.1 EU: Cybersecurity risk is a measure of the potential damage or loss a vulnerability could cause weighed against the likelihood an adversary will exploit the vulnerability.	7.1.1 LO: Students will be able to differentiate between threats, vulnerabilities, and attacks. 7.1.2 LO: Students will be able to identify and prioritize the protection of information assets. 7.1.3 LO: Students will create a threat model and evaluate the trade-offs associated with defending against different threat sources. 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.	7.1.1a EK: A vulnerability is a weakness or gap in a security program that can be exploited by threats to gain unauthorized access to an asset. 7.1.1b EK: A threat is anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. 7.1.1c EK: Attacks arise when threats exploit vulnerabilities. 7.1.2a EK: Information assets must be identified. 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. 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. 7.1.3a 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, capabilities/techniques, motivations, and aversion to risk. 7.1.3c EK: There are risks and solutions associated with closed/proprietary systems. 1.3.2a EK: Ethical obligations are covenants that define a moral course of action and draw a line between right and wrong. 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. 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. 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.

2: CIA Triad	2 Establishing Trust, 1 Ethics, 6 Adversarial Thinking, 5 System Security	2.1 EU Cybersecurity relies on confidentiality, integrity, and availability (the CIA triad).	2.1.1 LO: Students will evaluate methods of keeping information secret from those whom the information should be kept secret. 2.1.2 LO: Students will demonstrate that integrity involves trust and credibility. 2.1.3 LO: Students will evaluate methods of protecting information and information systems from disruption and destruction. 6.2.2 LO: Students will know how intentional attacks can adapt to defenses and cause a system to fail. 5.4.1 LO: Students will identify historical consequences of software and hardware vulnerabilities, e.g., power outages, death, theft of trade secrets from other sovereign nations.	2.1.1a EK: Confidentiality is the protection of information from disclosure to unauthorized parties. 2.1.1b EK: File permissions are a mechanism to control access to only those authorized. 2.1.1c EK: Cryptography is necessary to ensure confidentiality and integrity. 2.1.1d EK: Hiding is another aspect of confidentiality. 2.1.1e EK: Assuring confidentiality includes prevention, detection, containment, and response mechanisms. 2.1.2a EK: Integrity is the trustworthiness of data or resources. 2.1.2b EK: Assurance is determining how much and in which way to trust a system. 2.1.2c EK: Data integrity is the information changing in authorized ways by authorized people, often called authentication. 2.1.2d EK: Integrity mechanisms include prevention, detection and response mechanisms. 2.1.3aEK: Availability of information refers to ensuring that authorized parties are able to access the information when needed. 2.1.3b EK: Denial of service attacks are attempts to block availability. 2.1.3c EK: A disaster recovery plan (DRP) includes backups, redundancies, system dependencies, and alternate sites. 2.1.3d EK: Assuring availability includes prevention, detection, and response mechanisms. 1.2.1b EK: There are trade-offs concerning the harms and benefits of cybersecurity, including the tensions between ensuring privacy and enabling convenience and usability. 1.3.3c: EK Using the anonymity of the internet for behavior that can harm others may not be illegal. 6.2.2a EK: The intentions of adversaries can be classified as theft, disclosure, disruption, destruction, and/or subversion. 6.2.2b EK: The manner in which an adversary carries out their intentions (sometimes called attacks) is related to their capabilities and the resources they can bring to bear. 6.2.2c EK: Cyber systems are susceptible to attack from human adversaries. 6.2.2d EK: Incident response includes provisioning for the confidentiality, integrity and availability of cyber systems under attack by adversaries.

				5.4.1a EK: Software vulnerability examples that resulted in a loss of confidential data including breaches of credit information (Equifax), healthcare information (Anthem), government records (OPM data breach), home assistants (Amazon Echo hacks), baby monitors (many examples), and fitness tracker data (mapping military bases). 5.4.1b EK: Software vulnerability examples that resulted in a loss of confidential data and corresponding monetary losses for the victims including intellectual property theft and ability to directly access financial data. 5.4.1c: EK Software vulnerabilities examples that resulted in a loss of integrity such as man in the middle attacks (many examples), compromise industrial control systems (i.e. Stuxnet), vehicle control systems (Jeep Cherokee hack), and medical devices (Medtronic infusion pumps). 5.4.1d EK: Software vulnerability examples that resulted in a loss of availability such as DDoS attacks on websites (Mirai botnet), ransomware that locks outs access to data (WannaCry, Petya, NotPetya), Telephony Denial of Service (attacks on 911). 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.
3: What is Hard-ware and How Do Comput ers Work	5 System Securit y, 8 Implica tions	5.2 EU: Hardware security protects the machine and peripheral hardware from theft and from electronic intrusion and damage. 5.4 EU: Software and Hardware (or Systems) are everywhere which increasingly	5.2.1 LO: Students will convey that computer hardware refers to the physical parts of a computer and related devices. 5.4.1 LO: Students will identify historical consequences of software and hardware vulnerabilities, e.g., power outages, death, theft of trade secrets from other sovereign nations. 8.1.1 LO: Students will summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field.	5.2.1a EK: Internal hardware devices include motherboards, hard drives, memory, and internal peripherals such as a CD-ROM drive, CD-R drive, or internal modem. 5.2.1b EK: External hardware devices include monitors, keyboards, mice, printers, scanners, routers, switches, servers, IoT devices industrial control systems, security cameras. 5.2.1c EK: Hardware is the bottom level component of systems that are critical to telecommunications, health, US economic system, and national defense. 5.2.1d EK: Tamper resistant hardware aims to detect if someone attempts to modify them and aim to become non-functional if that occurs. For example, credit card readers at a store are designed to be no longer usable if someone physically opens the credit card reader system. 8.1.1a EK: Information campaigns were used and considered vital throughout history.

		makes it foundational in civilization.		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.
4: Cyber-security is Global	8 Implications, 1 Ethics	8.2 EU: Cybersecurity is global, transcending traditional boundaries, and is always evolving. 1.1 EU: Social goals reflect the foundational values held by society; these core societal values are reflected in cybersecurity choices.	8.2.1 LO: Students will describe how political ideologies, economic structures, social organizations, and cultural perceptions impact cybersecurity. 8.2.2 LO: Students will analyze how privacy concerns vary greatly in regards to societies, age, and socio-economic status. 1.1.1 LO: Students will analyze online and offline behaviors in societies, i.e., themselves, peers, families, communities, and countries, and deduce the values that govern these behaviors. 8.1.2 LO: Students will explain how the idea of the open internet led us to new innovations that impact our daily lives and our security.	8.2.1a EK: Nation states have various approaches to sovereignty, investment and deterrence regarding cyber technology. 8.2.1b EK: Cybersecurity is impacted by the state of a political alliance between nation states. 8.2.1c EK: Past and current laws are insufficient to assign blame for taking action that make our systems more vulnerable or to punish an entity for cyber crimes. 8.2.1d EK: To ensure the safety of a nation's critical infrastructure both public and private sectors are responsible for cybersecurity. 8.2.1e EK: Depending on the values of the entity, some will invest in research and development, while others invest in reverse engineering the work of others. 8.2.1f EK: Citizens in cyber space can more readily form ideological communities which is impacting what it means to be a nation state. 8.2.1g EK: Cultural perceptions and priorities of security may differ between countries affecting how and which security measures are implemented. 8.2.2a EK: Nation states have various approaches to civil rights and privacy regarding cyber technology. 8.2.2b EK: The combination of increasing power of new technology and the declining clarity and agreement on cybersecurity and privacy gives rise to problems concerning law, policy and ethics. 8.2.2c EK: When a government provides cybersecurity it can often lead to the reduction of privacy. 1.1.1a EK: Societies are groups of individuals characterized by common interests/values that are perpetuated by persistent social interaction. 1.1.1b EK: Cybersecurity ethics is an expression of values by the designers and users. 1.1.1c EK: Values concerning how to engage in cyber technologies can and do compete during the creative process of designing the technology and its adoption. 1.1.1d EK: Different communities and societies have different foundational social goals and values that impact their behaviors concerning technology.

				8.1.2a EK: The Internet provides global connectivity and is not structured around national boundaries. 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.
5: Cyber Law	4 Data Security, 1 Ethics, 8 Implications	4.2: Data Security uses non-technical and technical controls and techniques to protect data that is being processed, transmitted and stored.	4.2.1 LO: Students will compare and contrast data protection legislation, policies, and procedures that have been or are being introduced all over the world to protect personal data. 1.3.3 LO: Students will discuss how even when a cybersecurity practice is legal, it may not be ethical.	4.2.1a EK: Policies can be introduced and enforced at the local, state, and national levels. 4.2.1b EK: Laws are in place to protect the disclosure and misuse of financial, personal, and private information. 4.2.1c EK: GDPR (General Data Protection Regulation) is a set of regulations designed to give citizens in the European Union more control over their personal data. 4.2.1d EK: HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information. 4.2.1e EK: CFAA (Computer Fraud and Abuse Act) prohibits accessing a computer without authorization, or in excess of authorization. 4.2.1f EK: There are also state cybersecurity laws. One example are the Data Breach Disclosure laws that exist in 48 states, but differ by state. Another example is CCPA (California Consumer Privacy Act), which was signed into law in 2018 to extend the privacy rights of the citizens of California. 4.2.1g EK: An Acceptable Use Policy is a set of rules applied by the owner, creator or administrator of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used. 1.3.3a EK: The legal and ethical consequences of cybersecurity practices can be explored through ethical versus malicious hacking. 1.3.3b EK: Technology moves faster than laws can be created to govern it. 8.1.2c EK: Early government policies discouraged the use of encryption to build secure networks. 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.

6: Data Security Concerns	4 Data Security, 1 Ethics, 8 Implications	4.1 EU: Data security deals with the integrity of the data, i.e., the protection from corruption or errors; the privacy of data; and data confidentiality, i.e., it being accessible to only those who have access privilege to it. 4.2 EU: Data Security uses non-technical and technical controls and techniques to protect data that is being processed, transmitted and stored.	4.1.1 LO: Students will analyze existing data security concerns and assess methods to overcome those concerns. 1.2.1 LO: Students will discuss how cybersecurity can significantly impact the quality of people's lives both positively and negatively.	4.1.1a EK: Data can reveal much about people, their thoughts, and lives; which makes personally identifiable information highly sensitive. 4.1.1b EK: Data can be used to help individuals, but it can also be exploited to harm individuals. 4.1.1c EK: Data must be protected in processing, transmitting and storage. 4.1.1d EK: The purpose of personal data protection is not to merely protect a person's data, but to protect the fundamental rights, freedoms, and welfare of persons who are related to that data. 4.1.1e EK: Data integrity means only authorized changes are made only by authorized people. 4.1.1f EK: Origin integrity means the original data is trustworthy, and its source is trusted to produce trustworthy data. 4.1.1g EK: Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft. 1.2.1a EK: Examples in history demonstrate the harms and benefits of cybersecurity from multiple perspectives. 8.1.1c EK: Events in cyber warfare and cybercrime escalated the need for increased cybersecurity efforts. 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.
7: Principles of Software Design	2 Establishing Trust	2.2 EU: The simpler you can make the design or implementation of a system, the better you can check whether or not it can be exploited.	2.2.1 LO: Students will describe the principle of simplicity, which is about ensuring that systems are easy to understand, maintain and test so as to be more secure. 2.2.2 LO: Students will use the principle of abstraction to represent complicated concepts more simply and to allow solutions to be transferred to other contexts.	2.2.1a EK: Simple designs are easier to understand, maintain and test for security problems. 2.2.1b EK: Simplicity is also known as "Economy of Mechanism." 2.2.1c EK: A simple design incorporates a careful analysis of what is needed. 2.2.2a EK: Abstraction is reducing the complexity of an object down to its essentials in a way that is understandable. 2.2.2b EK: Good and elegant design involves using abstraction.

		2.3 EU: The more you restrict access, processes, resources, and users based on the policy, the more secure the system.	2.2.3 LO: Students will apply the principle of minimization by decreasing the number of ways in which attackers can exploit a program or device. 2.3.1 LO: Students will give examples of the principle of domain separation, which allows for the enforcement of rules governing the entry and use of domains by entities outside the domain. 2.3.2 LO: Students will know that the principle of process isolation prevents tampering or interference from/by other processes. 2.3.3 LO: Students will explain the importance of encapsulating resources, i.e., creating well-defined interfaces around resources to set rules for how the resources should interact. 2.3.4 LO: Students will explore the principle of least privilege, which is about differentiating among types of access control (mandatory, role-based, discretionary, and rule-based access controls) and analyzing which to use for selective restriction of access to a place or other resource. 2.3.5 LO: Students will break down how the principle of layering is a strategy for slowing down an attack because the attacker has to conquer each layer before moving on to the next. 2.3.6 LO: Students will know that the principle of data hiding is about	2.2.3a EK: The attack surface of a software environment is the sum of the different points where an unauthorized user can try to enter data or to extract data from an environment. 2.2.3b EK: Minimizing the attack surface decreases the opportunity to find an exploitable vulnerability in the system. 2.2.3c EK: The human interface should be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. 2.2.3d EK: Common mechanisms and access should be minimized. 2.3.1a EK: A domain refers to a collection of data or instructions that warrant protection. 2.3.1b EK: Communications between domains are allowed only as authorized. 2.3.2a EK: A process is a program running on a computer. 2.3.2b EK: Each process has a region of the memory (address space), which only it can access. 2.3.2c EK: Processes have to use defined communications mediated by the operating system to communicate with other processes. 2.3.3a EK: Examples of resources are the memory, disk drive, network bandwidth, battery power, and a monitor. It can also be system objects such as shared memory or a linked list data structure. 2.3.3b EK: Encapsulation allows access or manipulation of the class data in only the ways the designer intended. 2.3.4a EK: A privilege is a right for the user to act on managed computer resources. 2.3.4b EK: Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. 2.3.4c EK: Granting only those privileges necessary for a user to accomplish assigned duties improves accountability and limits accidental misuse. 2.3.5a EK: A layer is a separate level that must be conquered by an attacker to breach a system. 2.3.5b EK: Multiple independent layers require integration and independent management to get the full benefits of layered protection. 2.3.6a EK: Data hiding can help prevent users/programmers/processes from updating/changing data in invalid ways or by mistake.

			allowing only necessary aspects of a data structure or a record to be observed or accessed. 2.3.7 LO: Students will recognize that the cybersecurity often applies to a system that consists of individual self-sufficient components and the overall security is dependent on the security properties of the components. 2.3.8 LO: Students will define the principle of fail-safe defaults, which restricts how privileges are initialized when a subject or object is created.	2.3.7a EK: The principle of modularity says that individual components are capable of executing a unique part of the desired functionality and is achieved through system design. Because of this modular design, security upgrades can happen in one component without having to overhaul the entire system. 2.3.7b EK: A system's components may be separated and recombined. 2.3.8a EK: When something does not work or the system fails, the system must return to a secure state. 2.3.8b EK: A secure state is a condition when no subject can access any object in an unauthorized manner. 2.3.8c EK: Turning off permission causes a security problem. 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.
8: Cybersecurity Business Economics	8 Implications, 1 Ethics	8.3 EU: Measuring the economic value of cybersecurity is often an indirect process that relies on risk management trade- offs rather than direct benefits. 1.3 EU: Cybersecurity practices are highly complex and variable causing tensions between what the ethical duties are, to whom the ethical concern	8.3.1 LO: Students will explain how misaligned incentives encourage businesses to under invest in cybersecurity. 8.3.2 LO: Students will explain how economic forces influence the cybersecurity choices made by service providers and service designers. 8.3.3 LO: Students will describe how economics shape the decisions of consumers. 1.3.1 LO: Students will explore the tensions that exist between transparency, autonomy, resilience and security.	8.3.1a EK: Economic value typically measures gains achieved, not losses avoided. 8.3.1b EK: The lack of cybersecurity can cause substantial economic losses; including the compromise of sensitive data, the modification of critical data, the improper behavior of a system, or the unavailability of a system. 8.3.1c EK: The lack of cybersecurity can result in major financial and reputational loss, but this loss only occurs after a successful attack. 8.3.1d EK: Even in the event of a successful attack, the loss may or may not have lasting direct economic impact on the provider of the service. 8.3.1e EK: When misaligned incentives arise the party making the security–efficiency trade-off is not the one who loses out when attacks occur. 8.3.2a EK: Bolting on security after the design is completed is often driven by short term incentives such as cost, speed to market, and features that are immediately transparent to potential customers 8.3.2b EK: Building security into the design at the onset results in better long term security when compared with bolting security onto existing systems. 8.3.2c EK: Cybersecurity risks occur when outsourcing the production or maintenance of technology to third party sources that may have different security practices.

		should be considered, and whose interests should be invested in protecting.		8.3.2d EK: Whenever security depends on the weakest link in the global supply chain, firms do not prioritize in investing in security when they know that other players will not invest, leaving them vulnerable in any case. 8.3.3a EK: Consumers are often driven by new functionality which is tangible while the security features of the product may only be understood or appreciated when the security fails. 8.3.3b EK: In order to fully participate in today's economy, consumers must give away their data and agree to a company's terms that may conflict with their values 8.3.3c EK: Consumers are often unaware of the value of their information that they exchange for an incentive from a company that uses their data for monetary purposes. 8.3.3d EK: Ill-informed consumers and businesses are prone to underinvest or invest in wrong solutions if they do not possess an accurate understanding of threats and defenses. 1.3.1a EK: Transparency in cybersecurity is important for trustworthiness but can come at a risk to security. 1.3.1b EK: Autonomy is the idea that every entity is in control of their own thoughts and actions. 1.3.1c EK: Resilience is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. 1.3.1d EK: Security is freedom from potential harm or other unwanted coercive change caused by others. 8.1.1f EK: A loss of availability has disrupted critical business functions. 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.
9: Physical Controls	4 Data Security, 1 Ethics	1.2 EU: Ethical reflection and judgement are required in considering the potential harms, benefits, and trade-offs	4.2.2 LO: Students will identify physical controls that are used to secure data.	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. 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. 4.2.2c EK: Commonly used physical controls include: limited entry points, redundant systems, and surveillance cameras.

		involved in cybersecurity.		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.
10: Cryptography	4 Data Security, 8 Implications	4.3 EU: Cryptography techniques are necessary to keep data private and secure, and evolve with changes in technology. 8.1 EU: Cybersecurity shapes and is shaped by significant historical ideas and events.	4.3.1 LO: Students will define cryptography and explain how it is used in data security. 4.3.2 LO: Students will practice symmetric cryptosystems to send a message and explain how they work. 4.3.3 LO: Students will employ public key (asymmetric) encryption and explain how it works.	4.3.1a EK: Cryptography comes from two Greek words meaning "secret writing" and is the art and science of concealing meaning. 4.3.1b EK: Cryptanalysis is the breaking of codes. 4.3.1c EK: Cryptographic algorithms, also known as ciphers, which are mathematical functions used in the process of encryption and decryption. 4.3.1d EK: Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. 4.3.1e EK: Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. 4.3.1f EK: Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result. 4.3.1g EK: The primary goal of cryptography is to keep enciphered information secret. 4.3.1h EK: Symmetric encryption is a method of encryption involving one key for encryption and decryption. 4.3.1i EK: Public key encryption, which is asymmetric, is an encryption method that is widely used because of the enhanced security associated with its use. 4.3.1j EK: Hash functions can be used for checking whether a file was corrupted. 4.3.1k EK: Certificate authorities (CAs) issue digital certificates that validate the ownership. 4.3.2a EK: There are two basic types of symmetric ciphers: Transposition ciphers that diffuse the data in the plaintext and substitution ciphers that replace the data in the plaintext. 4.3.2b EK: In transposition ciphers the letters are not changed they are rearranged. The set of encryption functions E is simply the set of permutations of m, and the set of decryption functions D is the set of inverse permutations. 4.3.2c EK: Anagramming is a way to attack a transposition cipher. It uses tables of n-gram frequencies to identify common n-grams.

				4.3.2d EK: A substitution cipher changes characters in the plaintext to produce the ciphertext. 4.3.2e: A shift cipher is susceptible to a statistical ciphertext-only attack. 4.3.3a EK: Public key encryption does not require the sender and receiver to share the same key. 4.3.3b EK: Public key encryption uses a key pair – a private key known only to the entity and a cryptographically linked public key that can be shared with anyone. 4.3.3c EK: Secret messages encipher the message with the recipient's public key, are sent, and then the recipient can decipher it using their private key. 4.3.3d EK: Digital Signatures are a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate. 8.1.1d EK: The loss of confidentiality is a critical factor in warfare. 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.
11: Authentication and Identity Management	4 Data Security, 6 Adversarial Thinking, 2 Establishing Trust		4.2.3 LO: Students will evaluate and recommend technical controls that can be used to secure data. 6.1.4 LO: Students will understand how social behaviors and human factors impact the cybersecurity of a system design. 2.3.4 LO: Students will explore the principle of least privilege, which is about differentiating among types of access control (mandatory, role-based, discretionary, and rule-based access controls) and analyzing which to use for selective restriction of access to a place or other resource.	4.2.3a EK: Authentication is a process by which you verify that someone is who they claim they are. 4.2.3b EK: Authentication requires a database of information. 4.2.3c EK: Authentication can be done using multiple factors, something you have, something you know, something you do, & something you are. (E.g., have = card, know=password, do=sign, walk, are=fingerprint, retina) 4.2.3d EK: Identity management includes authentication, access control, sometimes coordination across different domains, and management of the credentials throughout the lifecycle. 4.2.3e EK: Passwords and passphrases are a common form of authentication. 4.2.3f EK: The strength of a password is a function of length, complexity, and unpredictability. 4.2.3g EK: Authorization is the process of establishing if the authenticated user, is permitted to have access to and/or act on a resource. 4.2.3h EK: Groups, Roles, Privileges and Permissions are used to manage authorization.

				4.2.3i EK: Access Control is the process of enforcing the required security for a particular resource. 4.2.3j EK: Failure to protect data can be due to faulty authentication, faculty authorization, and/or faulty access control. 6.1.4a EK: Human users of the system have their own conscious and unconscious objectives that can undermine cybersecurity protections and policies. 6.1.4b EK: Social engineering is one of the most widely used techniques in which an adversary compromises a system by convincing a human to violate the security policies in a way that enables the adversary to gain an advantage. 2.3.4a EK: A privilege is a right for the user to act on managed computer resources. 2.3.4b EK: Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. 2.3.4c EK: Granting only those privileges necessary for a user to accomplish assigned duties improves accountability and limits accidental misuse. 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.
12: Why is Soft-Ware Vulner-able?	7 Risk, 1 Ethics, 2 Establi shing Trust, 8 Implica tions	2.2 EU: The simpler you can make the design or implementation of a system, the better you can check whether or not it can be exploited.	7.2.3 LO: Students will be able to explain how the logical malleability of software and hardware can allow an adversary to change a system to meet the adversary's goals rather than the systems original objective. 1.2.2 LO: Students will give examples of where/how tools are used in ways that were not intended by the system designer. 2.2.1 LO: Students will describe the principle of simplicity, which is about ensuring that systems are easy to understand, maintain and test so as to be more secure.	7.2.3a EK: Software is frequently updated to correct both functional errors and security problems. 7.2.3b EK: Software changes could come from an adversary that intentionally inserts code to meet the goals of the adversary. 7.2.3c EK: Changes in software code are common and those introduced by an adversary are often not easily detected. 1.2.2a EK: The designer assumptions and user assumptions could differ. Another way to say this, the user may not know the assumptions of the designer for using the tool, leading the user to use the tool in a way the designer never intended. 2.2.1a EK: Simple designs are easier to understand, maintain and test for security problems. 2.2.1b EK: Simplicity is also known as "Economy of Mechanism." 2.2.1c EK: A simple design incorporates a careful analysis of what is needed.

			2.3.7 LO: Students will recognize that the cybersecurity often applies to a system that consists of individual self-sufficient components and the overall security is dependent on the security properties of the components.	2.3.7a EK: The principle of modularity says that individual components are capable of executing a unique part of the desired functionality and is achieved through system design. Because of this modular design, security upgrades can happen in one component without having to overhaul the entire system. 2.3.7b EK: A system's components may be separated and recombined. 8.1.1e EK: The violation of system integrity can alter the behavior of critical infrastructure. 8.1.2b EK: Security was not seen as a concern until much of the "infrastructure" for computer networks was in place. 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.
13: Soft-ware Vulner-abilities	5 System Securit y, 1 Ethics, 2 Establi shing Trust	5.3 EU: Security vulnerabilities in software are weaknesses in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.	5.3.1 LO: Students will describe common security-related software vulnerabilities. 5.3.2 LO: Students will identify the processes of developing secure software. 5.3.3 LO: Students will describe the process of validating that software remains secure through its lifecycle. 2.3.2 LO: Students will know that the principle of process isolation prevents tampering or interference from/by other processes.	5.3.1a EK: Injection attacks occur when an external source such as a user provides input that causes a program to behave in ways that violate the security policy by executing harmful commands. 5.3.1b EK: A buffer overflow is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations, and how this can be used as an entry point by an attacker to violate security policy. 5.3.1c EK: A software vulnerability may exist when data is allowed to include unauthorized control instructions that dictate how the program should behave and thus can cause the program to behave in a way that violates the security policy. 5.3.1d EK: A software vulnerability may exist when cryptographic functions are not implemented properly or when the cryptographic functions are assumed to provide more security than the algorithm provides. 5.3.1e EK: Changes to the environment can cause software to no longer meet the security policy and secure software must include considerations for how to implement future changes (e.g., credentials, algorithms, and patching code to correct bugs and errors). 5.3.1f EK: A software vulnerability can occur when external components that don't meet the security policy requirements are connected to the system.

				5.3.2a EK: Input validation is code added to the program that verifies input provided by an external source is the type of input expected and will be processed correctly. 5.3.2b: EK Static analysis of software is a process in which external tools analyze the code and automatically identify potential security vulnerabilities such as potential buffer overflows. 5.3.2c EK: Development tools and Integrated software Development Environments (IDE)s provide static analysis tools to check for some types of insecure code such as identifying potential buffer overflows. 5.3.3a EK: A security analysis is a process that is used to verify a program meets a specified list of security requirements. 5.3.3b EK: Security vulnerability reports such as Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE) are publicly available for software systems and should be monitored, or subscribe to their alerts. 5.3.3c EK: A zero day vulnerability is a software security flaw that is unknown to people who should be responsible for patching or fixing the flaw. 5.3.3d EK: Managing vulnerability reports, patching and patch distribution is a key part of software security. 5.3.3e EK: Dynamic analysis is a process in which external tools analyze the execution of code in order to automatically identify potential security vulnerabilities. 1.3.3d EK: Disclosure of software vulnerabilities to a party other than the software developer is legal and can be harmful. 2.3.2a EK: A process is a program running on a computer. 2.3.2b EK: Each process has a region of the memory (address space), which only it can access. 2.3.2c EK: Processes have to use defined communications mediated by the operating system to communicate with other processes. 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.
14: OSI Model	3 Ubiquitous Conne	3.1 EU: The Internet is a large, globally distributed	3.1.1 LO: Students will explain how devices use layers to communicate across the Internet and describe the purpose of the layers.	3.1.1a: EK Networks carry two types of information, those that allow for the controlling of the data and the data itself.

	ctivity, 2 Establishing Trust	network that is divided into layers, governed by protocols, and connects a wide variety of devices.	2.2.2 LO: Students will use the principle of abstraction to represent complicated concepts more simply and to allow solutions to be transferred to other contexts.	3.1.1b EK: Physical links include optical cables that send signals using light, cables that send signals using electrical pulses, and wireless networks that send signals over radio waves. 3.1.1c EK: Link layer protocols such as Ethernet, Wi-Fi (e.g., 802.11), and Bluetooth are specific to the physical layer connection and describe how the signals are used to exchange data between the devices. 3.1.1d EK: The network layer connects different types of physical/link layer networks into a single global Internet that transmits data from one computer to another using packets and logical addressing. 3.1.1e EK: Once a packet arrives at a device, the transport layer uses port numbers to determine which application (web browser, email app, game, etc.) receives the packet, allowing for the reliable delivery of data between a sending and receiving application. 3.1.1f EK: Internet and device applications (web, text messaging, games, etc.) follow protocols at the application layer (e.g. http, sms, proprietary protocols, etc.). 2.2.2a EK: Abstraction is reducing the complexity of an object down to its essentials in a way that is understandable. 2.2.2b EK: Good and elegant design involves using abstraction. 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.
15: Network Standards and Protocols	3 Ubiquitous Connectivity, 2 Data Security		3.1.2 LO: Students will explain how network standards and protocols allow different types of devices to communicate. 2.2.3 LO: Students will apply the principle of minimization by decreasing the number of ways in which attackers can exploit a program or device.	3.1.2a EK: Communication protocols define the rules, types, and formats of messages exchanged between devices and are necessary to allow devices to communicate with each other. 3.1.2b EK: One commonly used protocol is the Domain Name System (DNS) which provides a mechanism to map names like “www.example.com” into numbers (IP addresses), similar to a phonebook that maps names to phone numbers. 3.1.2c EK: Some protocols are proprietary and are available only to authorized users while other protocols are published as formal standards and allow devices from any manufacturer to communicate with each other. 3.1.2d EK: Some standards are open standards where the packet format and message exchange rules are available to everyone. In other standards called proprietary standards, the message formats and message exchange rules are only provided to authorized entities.

				3.1.2e EK: When designers rely on secrecy, assuming an adversary cannot compromise the system because the adversary cannot determine how the system works is known as security through obscurity. It is widely accepted that security through obscurity should never be your only security mechanism. 3.1.2f EK: Cryptographic algorithms are either publicly known or proprietary. The use of proprietary cryptographic algorithms is largely discredited, as evidenced by organizations like NIST, which encourages public review of algorithms. 3.1.2g EK: Through experiments, an adversary can often learn how proprietary protocols or algorithms work even though the adversary is not an authorized user. 2.2.3a EK: The attack surface of a software environment is the sum of the different points where an unauthorized user can try to enter data or to extract data from an environment. 2.2.3b EK: Minimizing the attack surface decreases the opportunity to find an exploitable vulnerability in the system. 2.2.3c EK: The human interface should be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. 2.2.3d EK: Common mechanisms and access should be minimized. 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.
16: Complexity of Cyberspace	7 Risk, 6 Adversarial Thinking	7.2 EU: There are factors that necessitate cybersecurity risk as emergent and complex: the presence of an adversary, the logical malleability of computers, and the decentralized	7.2.1 LO: Students will be able to explain how cyberspace is a very large, complex system of cybersystems that include hardware, software, social, economic, and political components. 6.1.1 LO: Students will explain how cybersystems are complex systems.	7.2.1a EK: A complex system is a system composed of many parts, which may interact with each other, where the interactions produce properties that its parts do not have. 7.2.1b EK: The behavior of complex systems has unpredictable output, i.e., it is intrinsically difficult to model due to the dependencies, competitions, relationships, or other types of interactions between the parts or between a given system and its environment. 7.2.1c EK: The behavior or output of cybersystems cannot be predicted simply by analyzing the parts and inputs of the system. 7.2.1d EK: The behavior of the system is emergent and changes with time. The same input and environmental conditions do not always guarantee the same output.

		and distributed nature of networked systems. 6.1 EU: Adversity comes from anyone or anything where the end result differs from that intended by the system designer and user.		7.2.1e EK: The participants or agents of a system (human agents, including or especially adversaries, in this case) are self-learning and change their behavior based on the outcomes of the previous experience. 6.1.1a EK: A complex system is a system composed of many components which may interact with each other. 6.1.1b EK: Complex systems typically have input from many sources and are highly changeable. 6.1.1c EK: The internet is a prime example of a complex system in that it is a large and complex system composed of multiple, dispersed, independent systems. 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.
17: Why is the Internet Vulnerable	3 Ubiquitous Connectivity, 1 Ethics	3.2 EU: The Internet provides a large attack surface, which offers efficiencies or economies of scale for adversaries.	3.2.1 LO: Students will analyze how the connected nature of the Internet allows an adversary to reach a large number of devices. 3.2.2 LO: Students will identify and predict the outcomes of security vulnerabilities at the physical/link layer, the network layer, the transport layer, and the application layer. 1.1.2 LO: Students will understand how the role of values and ethics affects political structures, laws, and policy decisions as it relates to cybersecurity	3.2.1a EK: Network mapping and recon tools allow an adversary to gain information on remote systems and an opportunity to get control of the system. 3.2.1b EK: By directing an attack at a collection of devices (or even all devices on a network), an adversary can attack multiple devices simultaneously, in hopes of compromising a few select devices. 3.2.1c EK: An adversary can attack a large number of systems simultaneously, which can impact a large majority of a group of people. 3.2.1d EK: An adversary can stay undetected for a long period of time suggesting that early detection is key in preventing a large amount of damage. 3.2.2a EK: At the physical/link layer, an adversary who is able to connect to the link can observe, and possibly modify or jam messages on that link. 3.2.2b EK: At the network layer, an adversary may do two things, impersonate an address (spoofing) or disrupt communications (Denial of Service). 3.2.2c EK: At the transport layer, an adversary may disguise their intentions by using port numbers incorrectly or may disrupt the ability of a device to deliver data to the application. 3.2.2d EK: At the application layer, messages sent by the adversary may cause applications to stop working or behave in a way that serves the goals of the adversary, rather than the way they were designed.

				1.1.2a EK: Political structure refers to institutions, their relations to and interactions with each other, and the laws and norms present in political systems in such a way that they constitute the political landscape of the political entity. 1.1.2b EK: Institution refers to informal norms, shared understandings, and formal doctrines that constrain and prescribe actors' interactions with one another. 1.1.2c EK: Cyberwarfare, cybersecurity and privacy affect and are affected by institutions, political structures and attendant policies. 1.1.2d EK: Cybersecurity laws reflect values about national security, economic security, welfare of citizens, domestic law and order, and legitimacy of government. 1.1.2e EK: Professional codes of ethics convey the expected conduct of cybersecurity professionals. 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.
18: Cyber Attack Chain	7 Risk, 6 Adversarial Thinking, 8 Implications		7.2.2 LO: Students will be able to describe how the presence of an adversary necessitates that cybersecurity risk is emergent and complex. 6.2.3 LO: Students will analyze how the cybersecurity attack lifecycle/kill chain is essential to adversarial thinking.	7.2.2a EK: Adversaries employ strategic reasoning, including where, when, and how they might attack, as well as tactics for evading detection. 7.2.2b EK: The steps in an attack are footprinting, scanning, enumeration, network mapping, gaining access, privilege escalation, implant, and hiding tracks. 7.2.2c EK: Adversaries are self-interested agents whose behavior evolves and adapts in response to their environments and other actors in the system. 6.2.3a: The term “kill chain” refers to the structure—or seven stages—of a cyberattack. 6.2.3b: Reconnaissance is the first stage in the attack lifecycle, where adversaries gather public information about the target, and scan their networks to identify how best to plan their attack. 6.2.3c: Weaponization is the second stage. Based on the information obtained through reconnaissance, the adversary will tailor their toolset to meet the specific requirements of the target network. This often includes coupling remote access with an exploit into a deliverable payload.

				6.2.3d: The third phase is delivery, which is the transmission of the weapon to the target environment using vectors like email attachments, phishing, websites, and removable media. 6.2.3e: Exploitation is the fourth phase where the code is triggered exploiting vulnerable applications or systems. 6.2.3f: The fifth stage is installation where attackers install a remote access trojan or backdoor on the victim system in order to conduct further operations, such as maintaining access, persistence and escalating privileges. 6.2.3g: Command and control is the sixth phase of the cyber kill chain. With malware installed, attackers now own both sides of the connection: their malicious infrastructure and the infected machine and can now actively control the system. Attackers will establish a command channel in order to communicate and pass data back and forth between the infected devices and their own infrastructure. 6.2.3h: The final stage of the kill chain is actions on the objective. Once adversaries have control, persistence, and ongoing command and communication, they will act upon their motivation in order to achieve their goal(s), e.g., data exfiltration, destruction of critical infrastructure, to deface web property, or to create fear or the means for extortion. 8.1.1g EK: The emergence of advanced persistent threats (APTs) have caused changes in the way individuals and companies are secured and who is involved in securing them. 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.
19: Network Security Technologies	3 Ubiquitous Connectivity, 6 Adversarial Thinking, 2 Establi		3.2.3 LO: Students will identify and distinguish between the purposes of network security devices and technologies. 6.1.2 LO: Students will explain how complexity impacts the failure of cybersystems. 2.3.5 LO: Students will break down how the principle of layering is a strategy for slowing down an attack because the attacker has to conquer	3.2.3a EK: Most protocols lack a security component but some protocols build in security. For example, http was designed before security was a major concern while extensions like https explicitly add security to the standard. 3.2.3b EK: A packet can be identified by its source address (sending device), source port (sending application on the device), destination address (receiving device), and destination port (receiving application on the device). 3.2.3c EK: Firewalls work primarily at the network and transport layer by blocking packets with addresses and ports that correspond to unwanted traffic.

	shing Trust		each layer before moving on to the next.	3.2.3d EK: Intrusion Detection Systems (IDS) work at all layers to identify and raise an alarm when unexpected message patterns (anomalies) or known bad patterns (signatures) are detected (blacklisting). IDS systems can also be configured to block all packets and only allow a select set of valid packets (whitelisting). 3.2.3e EK: Intrusion Prevention Systems (IPS) are similar to IDS and also can prevent attacks by blocking messages related to anomalies or signatures. 3.2.3f EK: Application layer defenses, such as input validation, check and block potentially harmful message data from getting to the application. 3.2.3g EK: Devices with limited processing power such as Internet of Things (IoT) devices and control systems in industrial settings may rely almost entirely on network security devices such as firewalls and IPS for protection. 6.1.2a EK: In complex systems, failures are rarely the result of one individual's problem or behavior; catastrophe requires multiple failures. 6.1.2b EK: System failures are characterized by a series of actions or behaviors that are normally isolated or self-contained, but become consequential due to interconnected impact. 6.1.2c EK: Product failure is deceptively difficult to understand given that it depends on the intrinsic properties of each part, what it's made of, how those materials respond to varying and unanticipated conditions, and how customers use a product. 6.1.2d EK: Given the complexity of cybersystems, there are limits to how much entities can control their functioning and success of their policies. 6.1.2e EK: Security is a characteristic of systems and not system components. 2.3.5a EK: A layer is a separate level that must be conquered by an attacker to breach a system. 2.3.5b EK: Multiple independent layers require integration and independent management to get the full benefits of layered protection. 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.
20: Network Meets	7 Risk, 2 Establi		7.2.4 LO: Students will be able to explain how the decentralized and dynamic nature of networked systems	7.2.4a EK: There are risks and mitigations associated with open systems like the Internet.

Crypto-graphy	shing Trust		create the potential for a system to fail or behave incorrectly due a component the designer didn't even know existed. 2.3.6 LO: Students will know that the principle of data hiding is about allowing only necessary aspects of a data structure or a record to be observed or accessed.	7.2.4b EK: Internet communication between a sender and receive relies on a number of systems that are not controlled by the sender or receiver. This can include the hardware and software at the sender and the sender's edge network. It includes a number of supporting systems such as the DNS and certificate authorities, and any number of intermediate networks. It can also include the receiver's edge network as well as the hardware and software at the receiver. 7.2.4c EK: Incorrect assumptions about the network can result in the loss of confidentiality by sending data to an imposter or sending data over a path where it can be observed. 7.2.4d EK: Network vulnerabilities can result in the loss of integrity if data is sent to an imposter acting as a "monkey-in-the-middle" or when data is sent over a path where it can be changed. 7.2.4e EK: Network vulnerabilities can result in the loss of availability by directing the sender to an invalid destination or sending data over a path where it can be dropped. 7.2.4f EK: Cryptography can be used to prevent imposters and protect data so only authorized entities can view it. 7.2.4g EK: Cryptography can be used to identify the creator of a message and show a message was not modified in transit (hash function). 7.2.4h EK: Certificate authorities play a role in asserting the identities. 7.2.4i EK: Cryptography does not solve operational challenges and cryptography alone is not a solution in a decentralized network. 2.3.6a EK: Data hiding can help prevent users/programmers/processes from updating/changing data in invalid ways or by mistake. 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.
21: Hardwar e and Software Integrati on	5 System Securit y, 2 Establi shing Trust	5.1 EU: Systems consist of a combination of hardware and software that together achieve some objective and security requires	5.1.1 LO: Students will identify how hardware and software work together in complex ways to achieve an overall objective. 2.3.1 LO: Students will give examples of the principle of domain separation, which allows for the enforcement of rules governing the entry and use of	5.1.1a EK: Software is a set of instructions that execute on hardware and are designed to achieve some objective on a physical device. 5.1.1b EK: Neither hardware or software is useful without the other. 5.1.1c EK: Software instructions may manipulate data, manipulate physical systems or manipulate both. For example, software in a vehicle may record the vehicle speed and send it to a cloud storage system, other software may cause the brakes to be physically applied and reduce the speed, and still other software may both record and manipulate the vehicle speed.

		integration of both.	domains by entities outside the domain.	5.1.1d EK: Malware, short for malicious software, is any software intentionally designed to cause damage to a computer, server, client, or computer network. 5.1.1e EK: Software includes programs written to run on servers, laptops, and traditional computers. Computing devices accomplish no tasks without running software that tells it what to do. 5.1.1f EK: Software can be written in high level languages such as Python, C, Perl, Java and the high level software is converted into low level instructions that tell the CPU, memory, and other devices exactly what to do. 5.1.1g EK: Software can be written in low level machine specific instructions that tell the CPU, memory, and other devices exactly what to do (e.g. add memory locations one and two and store the result in memory location. 5.1.1h EK: Embedded software can be built directly into the physical device so the instructions on how a device will behave are physically part of the device and often cannot be changed without changing the hardware itself. 5.1.1i EK: Embedded software is computer software, written to control machines or devices that are not typically thought of as computers, commonly known as embedded systems. 5.1.1j EK: Software ultimately relies on the physical hardware to accomplish its task and even if the software is written perfectly, it will not perform the desired function if the hardware fails to behave as expected. In other words, the software may correctly instruct the hardware to add two numbers and store the result in memory location 3. If memory location 3 has an error or vulnerability and does not store the correct value, the software will not accomplish its objective. 5.1.1k EK: Hardware ultimately relies on the software instructions to accomplish its task and even if the hardware operates perfectly, it will not perform the desired function if the software fails directs it to execute the wrong instructions. In other words, the hardware may be able to correctly apply the brakes in a vehicle when instructed to do but it will not prevent a vehicle crash if the software is too slow in deciding when to apply the brakes.

				5.1.1l EK: The overall system can be manipulated to act incorrectly if there is a vulnerability in the hardware, the software, the interface between them, or any combination of those. 2.3.1a EK: A domain refers to a collection of data or instructions that warrant protection. 2.3.1b EK: Communications between domains are allowed only as authorized. 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.
22: Common Hardware Vulnerabilities	5 System Security, 7, Risk, 2 Establishing Trust		5.2.2 LO: Students will know some common hardware-related vulnerabilities. 5.2.3 LO: Students will describe the process of developing secure hardware and validating that it is secure through its lifecycle. 5.2.4 LO: Students will identify hardware security addresses issues related to an adversary physically gaining access to a device. 2.3.3 LO: Students will explain the importance of encapsulating resources, i.e., creating well-defined interfaces around resources to set rules for how the resources should interact.	5.2.2a EK: A backdoor is a method, often secret, of bypassing normal authentication or encryption in a computer system, a product, or an embedded device (e.g. a home router) to secure remote access. 5.2.2b EK: Manufacturing backdoors are used for malware or other penetrative purposes; backdoors aren't limited to software and hardware, but they also affect embedded radio-frequency identification (RFID) chips and memory. 5.2.2c EK: A side channel attack is based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs) 5.2.2d EK: General classes of side channel attacks include attacks such as: timing attacks, power-monitoring attacks, electromagnetic attacks, data remanence attacks. 5.2.2e EK: Hardware vulnerabilities can also be due to weaknesses in the implementation of algorithms. 5.2.3a EK: Hardware itself consists of many components and supply chain management attempts to ensure each component as well as the composition of these components meets an overall security policy. 5.2.3b EK: The hardware design, manufacturing and supply chain can be attacked by malicious actors, nation states, competitors, and organized crime. 5.2.3c EK: Physical security measures can be used to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm. 5.2.4a EK: The hardware design can require the device disable itself if physically tampered.

				5.2.4b EK: Students will identify examples of fail-safe in cybersecurity, i.e., a design feature or practice that in the event of a specific type of failure, inherently responds in a way that will cause no or minimal harm to other equipment, the environment or to people and provide recovery opportunities. 7.2.3d EK: Hardware itself may act in unintended ways and an adversary is seeking to find and exploit these unintended behaviors. 2.3.3a EK: Examples of resources are the memory, disk drive, network bandwidth, battery power, and a monitor. It can also be system objects such as shared memory or a linked list data structure. 2.3.3b EK: Encapsulation allows access or manipulation of the class data in only the ways the designer intended. 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.
23: Conducting Security Testing and Assessments	7 Risk, 1 Ethics, 6 Adversarial Thinking	6.2 EU: Adversarial thinking is the process of reasoning about how opposing forces could prevent a system from meeting both its functional and security goals.	7.1.4 LO: Students will be able to conduct standard security testing and assessments. 7.1.5 LO: Students will understand the trade-offs between cybersecurity benefits and the total cost of cybersecurity protections. 6.2.1 LO: Students will know how natural events and unintentional errors can cause a system to fail.	7.1.4a EK: Vulnerability assessment identifies known vulnerabilities on the system. 7.1.4b EK: Known vulnerabilities can be found in databases that collect, maintain, and disseminate information. 7.1.4c EK: There are various automated vulnerability scanning tools, which are used for pinpointing vulnerabilities and providing remediation for these vulnerabilities. 7.1.4d EK: Not all vulnerabilities can be exploited and not all vulnerabilities need to be mitigated. 7.1.4e EK: Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. 7.1.5a EK: The outcome of a risk assessment should prioritize what needs to be remediated. 7.1.5b EK: If the data or resources cost less or are of less value than their protection, adding security mechanisms is not cost effective. 7.1.5c EK: The level of protection is a function of the attack occurring and the effects of the attack should it succeed. 1.2.2b EK: Security tools were designed to help system administrators and users to improve security, but an adversary can use the same tools to exploit the target for nefarious goals.

				6.2.1a EK: Cyber systems are susceptible to disruption and destruction from natural disasters; for example, flooding, earthquakes, and hurricanes. 6.2.1b EK: Disaster planning includes provisioning for the confidentiality, integrity and availability of cyber systems during natural disasters. 6.2.1c EK: Disaster planning includes prevention, detection, and response and recovery. 6.2.1d EK: Natural event and unintentional errors typically do not adapt in response to defenses. 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.
24: Cyber Physical Systems	5 System Security, 2 Establishing Trust, 8 Implications		5.4.2 LO: Students will predict how physical systems that rely on software may be vulnerable to future attacks. 2.3.8 LO: Students will define the principle of fail-safe defaults, which restricts how privileges are initialized when a subject or object is created.	5.4.2a EK: A cyber-physical system (CPS) is a mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users. 5.4.2bEK: Industries that employ CPS include energy management, health care, manufacturing, transportation, telecommunications, infrastructure, and military. 5.4.2c EK: A smart grid is an electrical grid which includes a variety of operation and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficient resources. 5.4.2d EK: Increased industry connectivity will cause increased attacks from adversaries such as cyber criminals, disgruntled employees, terrorists, organized crime, and nation states. 5.4.2e EK: Vulnerabilities may allow adversaries to interfere with connected devices. 5.4.2f EK: The consequences of unintentional faults or malicious attacks could have severe impact on human lives and the environment. 5.4.2g EK: By targeting trusted resources attackers can control devices and wholeheartedly manipulate users. 2.3.8a EK: When something does not work or the system fails, the system must return to a secure state. 2.3.8b EK: A secure state is a condition when no subject can access any object in an unauthorized manner 2.3.8c EK: Turning off permission causes a security problem. 8.1.2d EK: The Internet has evolved to include new types of devices and the “Internet of Things."

				8.1.2e EK: The "Internet of Things," benefits our daily lives by providing easier access to information, the ability to offload menial tasks, and coordinate necessary information. 8.1.2f EK: The Internet and IoT devices create new vulnerabilities an adversary can exploit. 8.1.2g EK: The increasing dependence on the Internet and IoT devices introduces problems when these systems become unavailable. 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.
25: Design Trade-offs	2 Establishing Trust, 1 Ethics, 6 Adversarial Thinking, 8 Implications	2.4 EU: Identifying and questioning assumptions is a key part of making a system more secure.	2.4.1 LO: Given a scenario, students will identify the assumptions made in the design of the system, evaluate their impact on security, and consider how different assumptions change the security. 6.1.3 LO: Students will understand how different system components impact the cybersecurity of a system design.	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. 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. 2.4.1c EK: Incorrect assumptions lead to system failures. 2.4.1d EK: When confronting incorrect assumptions, facing up to cyber attacks is an ongoing, and constantly evolving challenge. 2.4.1e EK: The only assumption you can safely make is that data and networks are not safe. 1.2.1c EK: Cybersecurity requires resources, including time, money, and expertise that also affects technological affordances. 6.1.3a EK: Security is only as strong as the weakest link and is not limited to human actors. 6.1.3b EK: Human operators have dual roles: as producers and defenders against failure. 6.1.3c EK: Events ranging from natural disasters to unintentional errors can result in cybersecurity failures. 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.

Pacing

Unit	Hours of Instruction	Unit Summary
1. What Is Cybersecurity	5	Students will explore the concept of cybersecurity. They will differentiate between threats, vulnerabilities, and attacks. They will also discuss information assets and discuss risk to those assets. Ethics and careers are also discussed in this unit.
2. CIA Triad	8	Building on the definition of cybersecurity, this unit explores the CIA triad. This unit also covers ethics, the consequences of a cyber-attack, and historic examples of such attacks.
3. What Is Hardware and How Do Computers Work	7	This unit defines a computer and its fundamental components. They will also understand the function of the components and how they connect together.
4. Cyber Is Global	7	In order for student to understand the global implications of cybersecurity, this unit has students compare and contrast the state of cybersecurity across the globe, paying attention to how attitudes differ among societies, age, etc.
5. Cyber Law	6	Starting with the difference between criminal and civil law, students will explore cybersecurity related legislation and polices on a federal and state level. Students will learn how computers are used in crime, the role of acceptable use policies, and the concept of ethical hacking.
6. Data Security Concerns	6	Data security concerns, including non-technical and technical controls, are taught in this unit. Cyber warfare is used to demonstrate data security concerns. Origin integrity is

		discussed, along with how cybersecurity impacts a person's quality of life.
7. Principles of Software Design (Overview)	5	This unit provides a quick introduction to the principles of software design. These concepts are explored in detail in later units.
8. Cybersecurity Business Economics	7	The need for baked-in versus bolted-on security is stressed in this unit. Here, students explore the reasons individuals and businesses under invest in cybersecurity, research the consequences of this choice, and learn about vulnerabilities tied to a global attack chain. Strategies for resiliency are also discussed.
9. Physical Controls	5	Before digging deeper into technical controls in later units, this unit focuses on physical controls. Building on the idea of defense in depth covered in earlier chapters, this unit encourages students to build their own cyber fortress through limited entry points, redundant systems, and surveillance.
10. Cryptography	9	Starting with hands-on historic symmetric ciphers, this unit demonstrates the impact of cryptography on warfare. It then explains the different modern algorithms, progressing to hashing functions, public key encryption, and digital certificates.
11. Authentication & Identity Management	7	User credentialing is an important part of cybersecurity. Students will master this concept through studying the numerous options of user authentication, including something you have, know, do, or are. Students will also consider the strengths and weaknesses of each type and discuss the benefits of multi factor authentication. The unit ends with a study on social engineering, authorization, and least privilege.
12. Why Is Software Vulnerable	6	Bug hunting becomes a topic of interest as learners translate what they know about baked-in versus bolted-on security into the area of software design. Patch management is discussed, as well as designer and user assumptions. Students also gain a deeper understanding of modularity and simplicity.

13. Software Vulnerabilities	10	Building on topics from the previous chapter, students look at the technical side of software vulnerabilities. From buffer overflows to zero day attacks, the unit covers security-related software vulnerabilities and how to avoid them through security software development. Process isolation is explored in greater detail.
14. OSI Model	8	All People Seem To Need Data Processing. This lesson traces a packet through the OSI model. Students also focus on abstraction.
15. Network Standards & Protocols	8	Using their connections to the OSI model, students will learn about various devices' standards and protocols. Students will also learn more about minimization.
16. Complexity of Cyber Space	7	Taking concepts from previous units, students will tie the knowledge together to appreciate the complexity of cyber space. Not only will students visualize the size and complexity of cybersystems, they will also have a better understanding of adversaries.
17. Why Is the Internet Vulnerable	7	Once students understand the complexity of cyberspace, they will map the Internet as an attack surface. Drawing from previous lessons, the students will contrast ethics with the various ways the Internet can be attacked.
18. Cyber Attack Chain	6	After seeing the ways the Internet is vulnerable, the learners will trace the steps of a cyber-attack. Starting with reconnaissance and ending with covering his/her tracks, the students will see how individuals and businesses defend against advanced persistent threats.
19. Network Security Technologies	7	Network defense is the topic of this unit. Students become familiar with all the tools available to protect attackers. This unit covers the tools individually and then asks students to apply the principle of layering to see how the tools can work together.
20. Network Meets Cryptography	5	Drawing from their understanding of network security, students will see where cryptography fits into network security. Here, data protection through data hiding is the focus.

21. Hardware & Software Integration	10	The unit explores the interrelationship between hardware and software. It offers a transition between software vulnerabilities studied previously and hardware vulnerabilities studied in the next unit. It details embedded systems and hardware's reliance on software for instructions. Domain separation is a design principle covered in this unit.
22. Common Hardware Vulnerabilities	8	Looking through the context of a backdoor, students explore how attackers bypass normal authentication and encryption. They also learn about RFID and side channel attacks. Students will tie this to supply chain topics covered earlier in the curriculum.
23. Conducting Security Testing & Assessments	12	Building upon the knowledge of vulnerabilities taught throughout the curriculum, this unit familiarizes students with conducting standard security testing and assessments. It also shows how adversaries can use the same tools to target systems.
24. Cyber Physical Systems	9	Students will take the cybersecurity knowledge they have gained from previous units and apply the concepts to cyber physical systems. Here, coming full circle from the curriculum's introduction, students will see how attackers can leverage exploits to attack a nation's infrastructure. As the world's dependence on IoT grows, so does the impact of such an attack.
25. Design Trade-offs	5	This concluding unit stresses that security is only as strong as the weakest link. It reminds students of humanity's dual role as producers and defenders. Additionally, it addresses additional threats to a system, such as natural disasters, change, and human error.

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.

UNIT 2: CIA Triad

Estimated Time in Hours: 8

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 6 Adversarial Thinking 1 Ethics 5 System Security	2.1	- Research history breaches and tie them to confidentiality, integrity, and availability.

Guiding Questions:

- What is the CIA triad, and why is it important?
- Who/what threatens CIA?
- Why do we need CIA?
- How do we protect confidentiality, integrity, and availability?
- What needs integrity?
- What do businesses do when systems go down?
- What is the CIA tradeoff?
- What's legal?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
2.1 EU Cybersecurity relies on confidentiality, integrity, and availability (the CIA triad).	• Computer, lecture slides, projector, graphic organizers • "Sneakers (4/9) Movie CLIP - No More Secrets (1992) HD." *YouTube*, uploaded by Movieclips, 29 May 2011, https://www.youtube.com/watch?v=F5bAa6gFvLs&feature=emb_logo	• Show movie clip from *Sneakers* linked left. What were the hackers trying to gain access to? What would happen if someone gained control of these things in real life? Point out that the Federal Reserve attack is a loss of confidentiality, the power grid attack is a loss of availability, and the air traffic control attack is a loss of availability. • These three things (confidentiality, integrity, and availability) are what cybersecurity experts try to protect. They compose the CIA triad. • Show the video linked left to introduce the CIA triad.

	• "What is the CIA Triad?" *YouTube*, uploaded by Netwrix, 25 February 2019, https://www.youtube.com/watch?v=xtlFO8Q2GDQ&feature=emb_logo	
6.2.2b EK: The manner in which an adversary carries out their intentions (sometimes called attacks) is related to their capabilities and the resources they can bring to bear. 6.2.2a EK: The intentions of adversaries can be classified as theft, disclosure, disruption, destruction, and/or subversion.	• "CIA Triad." *Quizizz*, created by kimswhite, 2019, https://quizizz.com/admin/quiz/5d6543fd91225c001d7bf45a/cia-triad	• Ask students to list thing that threaten the CIA triad. Be sure to note that these threats include natural disasters, human error, and attackers. • What types of attackers do they know about? Possible answer: nation states, hacktivist, criminals, insider threats, and script kiddies. Review these categories. • Have students list the motivations of these adversaries (see 6.2.2a EK). • Have students play the Quizizz game linked left.
2.1.1a EK: Confidentiality is the protection of information from disclosure to unauthorized parties 2.1.1 LO: Students will evaluate methods of keeping information secret from those whom the information should be kept secret	• Cichonski, Millar, Grance, and Scarfone. "Computer Security Incident Handling Guide; Recommendations of the National Institute of Standards and Technology." SP 800-61 Rev. 2, *NIST*, https://nvlpubs.nist.gov/nistpubs/SpecialPublica	• Have students discuss things they want to keep confidential. How do they keep these things confidential? • Discuss prevention, detection/analysis, containment, and post-incident activities. The booklet linked left is an excellent resource for this and could be used for a jigsaw activity or group research project. • Note that controls are ways to secure confidentiality. These include physical, technical, and administrative controls.

2.1.1e EK: Assuring confidentiality includes prevention, detection, containment, and response mechanisms. 2.1.1 LO: Students will evaluate methods of keeping information secret from those whom the information should be kept secret 2.1.1b EK: File permissions are a mechanism to control access to only those authorized. 2.1.1c EK: Cryptography is necessary to ensure confidentiality and integrity. 2.1.1d EK: Hiding is another aspect of confidentiality.	tions/NIST.SP.800-61r2.pdf • "Steganography Online." *GitHub*, created by stylesuxx, 2014, http://stylesuxx.github.io/steganography/	• Explain that file permissions are an example of a technical control. Provide examples of this. • Another technical control is cryptography. Explain the definition and purpose of cryptography. • Another way to keep information confidential is data hiding. Steganography is an example of this. There are many online tools available that can be used for steganography. One of those tools is linked left. It is a good idea to create examples of steganography for students to find. These can later be compared to the originals by hashing the files (when integrity is covered).
2.1.2a EK: Integrity is the trustworthiness of data or resources. 2.1.2d EK: Integrity mechanisms include prevention, detection and response mechanisms.		• Ask students if they have ever heard of someone pretending to be someone different online. Is this okay? Why or why not? When a person does this, they lose integrity. Explain the concept of integrity. • What are some other things that we want to be able to trust (files, processes, and systems)?

2.1.2c EK: Data integrity is the information changing in authorized ways by authorized people, often called authentication. 2.1.2 LO: Students will demonstrate that integrity involves trust and credibility. 2.1.2b EK: Assurance is determining how much and in which way to trust a system.		• Discuss ways that files, processes and systems can lose integrity. Cover integrity mechanisms with students (prevention, detection, and response). • A hashing exercise is a good activity here. Discuss ways people authenticate into a system.
2.1.3 LO: Students will evaluate methods of protecting information and information systems from disruption and destruction. 2.1.3aEK: Availability of information refers to ensuring that authorized parties are able to access the information when needed. 2.1.3b EK: Denial of service attacks are attempts to block availability.	• Cichonski, Millar, Grance, and Scarfone. "Computer Security Incident Handling Guide; Recommendations of the National Institute of Standards and Technology." SP 800-61 Rev. 2, *NIST.gov*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf • Schwartz, Samantha Ann. "Black Friday traffic brings down J. Crew, Ulta sites,	• Ask students about a time when they lost Wi-Fi, cell service, or access to a resource (crashed website). How did it impact them? Explain that availability is also important. • Describe a denial of service (DoS) attack. • Have students list ways to defend against a DoS attack. • Using the NIST Computer Security Incident Handling Guide, have students research each stage (as mentioned above). Have students notice that prevention, detection, and response help assure availability. • Have students read the article linked left. How does being down impact online retailers?

2.1.3 LO: Students will evaluate methods of protecting information and information systems from disruption and destruction. 6.2.2d EK: Incident response includes provisioning for the confidentiality, integrity and availability of cyber systems under attack by adversaries. 2.1.3c EK: A disaster recovery plan (DRP) includes backups, redundancies, system dependencies, and alternate sites. 2.1.3d EK: Assuring availability includes prevention, detection, and response mechanisms. 1.2.1b EK: There are trade-offs concerning the harms and benefits of cybersecurity, including the tensions between ensuring privacy and enabling convenience and usability. 6.2.2 LO: Students will know how intentional attacks can adapt to	among other retailers." *CIO Dive*, 26 Nov. 2018, https://www.ciodive.com/news/black-friday-traffic-brings-down-j-crew-ulta-sites-among-other-retailers/542926/ • *Cyberthreat Real-Time Map*. Kaspersky, https://cybermap.kaspersky.com/	• Discuss tradeoffs related to the CIA triad. Have students list examples. • Explore the threat map linked left with students. Explain that systems are constantly under attack and that adversaries are constantly adapting and changing their tactics, making CIA even harder to maintain.

defenses and cause a system to fail.		
1.3.3c: EK Using the anonymity of the internet for behavior that can harm others may not be illegal. 6.2.2c EK: Cyber systems are susceptible to attack from human adversaries. 5.4.1 LO: Students will identify historical consequences of software and hardware vulnerabilities, e.g., power outages, death, theft of trade secrets from other sovereign nations. 5.4.1a EK: Software vulnerability examples that resulted in a loss of confidential data including breaches of credit information (Equifax), healthcare information (Anthem), government records (OPM data breach), home assistants (Amazon Echo hacks), baby monitors (many examples), and fitness tracker data (mapping military bases).		• Another problem impacting CIA is the fact that laws are different all over the world. In some cases, adversaries in other countries are not breaking the law in their home country. • Also, adversaries target more than just desktops and laptops. They target various types of cyber systems. Provide students of examples of this. • Have students research the examples listed in EKs 5.4.1a-5.4.1d, noting how they impacted CIA. This would be a great poster activity.

5.4.1b EK: Software vulnerability examples that resulted in a loss of confidential data and corresponding monetary losses for the victims including intellectual property theft and ability to directly access financial data. 5.4.1c: EK Software vulnerabilities examples that resulted in a loss of integrity such as man in the middle attacks (many examples), compromise industrial control systems (i.e. Stuxnet), vehicle control systems (Jeep Cherokee hack), and medical devices (Medtronic infusion pumps). 5.4.1d EK: Software vulnerability examples that resulted in a loss of availability such as DDoS attacks on websites (Mirai botnet), ransomware that locks outs access to data (WannaCry, Petya, NotPetya), Telephony Denial of Service (attacks on 911).		

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.		• Invite a local cybersecurity professional to showcase their career to your classroom. Hold a Q&A session for the students.

UNIT 3: What Is Hardware and How Do Computers Work?

Estimated Time in Hours: 7

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
5 System Security 8 Implications	5.2, 5.4	- Practice building a computer from scratch using old computer desktop hardware. - Research computer hardware and plan a compatible computer system for a specific task (gaming, computation, light office use, etc.) using PCPartPicker. - Practice converting numbers between decimal and binary. Optionally, introduce Internet of Things (IoT as another type of computer system being integrated with society.

Guiding Questions:

- What are the individual parts of a computer? What is the role of each?
- What is external hardware, and how does it differ from internal hardware?
- Is hardware in all computer systems?
- Why are binary numbers, 0's and 1's, so important for computers?
- How is hardware present in infrastructure, military systems, hospitals, etc.?
- How can hardware be protected?
- What are information campaigns, and do they benefit or harm society?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
5.2.1a EK: Internal hardware devices include motherboards, hard drives, memory, and internal peripherals such as a CD-ROM drive, CD-R drive, or internal modem.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Graphic organizer for internal hardware components.	• Be sure to describe the basic function of each internal hardware component (CPU, GPU, HDD/SSD, RAM, Motherboard, PSU, etc.). • Pair with a computer hardware graphic organizer to let students label where internal hardware is while they learn about the specific components.

	• Old computer desktops for students to take apart and reassemble in a guided activity. Your school's IT dept or community may have these available. Phillips screwdrivers and safety measures are required for this activity. • Computer Hardware: "What does what in your computer? Computer parts Explained." *YouTube*, uploaded by Basics Explained H3Vtux, 17 Jan 2018, https://www.youtube.com/watch?v=ExxFxD4OSZ0 • Kahoot!	• Show students the summary video of internal hardware function. • Review internal hardware identification and function using Kahoot!.
5.2.1c EK: Hardware is the bottom level component of systems that are critical to telecommunications, health, US economic system, and national defense.	• Flippy-do: "CS Principles 2018 | Unit 1 | Ch. 1| Lesson 5: Binary Numbers." *Code.org*, https://curriculum.code.org/csp-18/unit1/5/ • Binary blitz: "Binary Blitz." *Penjee*,	• Teach binary structured as a bottom level component of computers. • Task students with paper-crafting a flippy-do to help them convert between binary and decimal notation. • Challenge the students with Binary blitz, a web-based binary conversion game with score tracking. Once they are familiar with the game, give the class 1 minute to earn as

	https://games.penjee.com/binary-numbers-game/index.html • IoT Introduction: "What is the Internet of Things?" *YouTube*, uploaded by GCFLearnFree.org, 19 July 2017, https://youtu.be/EKRVILAohck	many points as possible in a competition. Alternatively, students can work to earn points together to achieve a class-wide prize. • Later in the unit, expand on the criticality of hardware system. Discuss with students how computer hardware can be found in critical systems like military, infrastructure, and financial. • IoT can also be introduced here. Ask students how IoT might impact daily lives in the future, whether those are positive or negative impacts, and what some cybersecurity concerns are with IoT. Optionally, they can research different technologies that may make IoT secure/vulnerable.
5.4.1 LO: Students will identify historical consequences of software and hardware vulnerabilities, e.g., power outages, death, theft of trade secrets from other sovereign nations.	• Info about Meltdown and Spectre: "Meltdown and Spectre." *meltdownattack.com,* https://meltdownattack.com/ • Meltdown demo (spying on passwords): "Spectre & Meltdown – Computerphile." *YouTube*, uploaded by Computerphile, 5 Jan 2018, https://youtu.be/I5mRwzVvFGE	• Introduce the concept of hardware vulnerabilities and challenge the students to identify hardware vulnerabilities, or challenge them to describe why scenarios are considered to have hardware vulnerabilities. • Use Meltdown and Spectre as recent examples. • Introduce the Stuxnet attack here. You can pivot this example into 8.1.1 LO.

	• Graphic of how Stuxnet worked: "How Stuxnet Worked." *IEEE Spectrum*, 2013, http://farm9.staticflickr.com/8371/8515879321_b323dd534f_b.jpg	
5.2.1b EK: External hardware devices include monitors, keyboards, mice, printers, scanners, routers, switches, servers, IoT devices industrial control systems, security cameras.	• Kahoot!	• Discuss types of external hardware: this is probably familiar to most of the class. • Use Kahoot! to review external hardware alongside internal hardware. Students should be familiar with these terms and how to classify hardware.
5.2.1d EK: Tamper resistant hardware aims to detect if someone attempts to modify them and aim to become non-functional if that occurs. For example, credit card readers at a store are designed to be no longer usable if someone physically opens the credit card reader system.		• Provide examples of tamper resistance in the real world (security stickers, bottle seals) and how it relates to computers (cable lock, backup power). • Task the students with researching tamper resistant devices.
8.1.1 LO: Students will summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field.		• Revisit Stuxnet as a major cyber attack and ask students why they think it was such a big deal. Stuxnet was a prime example of what cyber warfare can resemble.

		• You can task students with researching news articles about Stuxnet or attacks against infrastructure.
8.1.1a EK: Information campaigns were used and considered vital throughout history.	• Deepfake video example: "Full House of Mustaches – Nick Offerman [deepfake]." *YouTube*, uploaded by DrFakenstein, 11 Aug 2019, https://youtu.be/aUphMqs1vFw	• Introduce information campaigns and the concept of propaganda. Relate this to promoted social media content and advertisements. • Ask the students to list examples of information campaigns they have seen and the purpose of them. • Show your class deepfake videos on YouTube and ask them to discuss the repercussions.
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.		• Discuss a relevant career, such as computer technician or computer engineer.

UNIT 4: Cybersecurity Is Global

Estimated Time in Hours: 7

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
8 Implications 1 Ethics	8.2, 1.1	- Learn how the Internet has evolved and how it impacts today's society. - Research things that impact cybersecurity.

Guiding Questions:

- What was life like before the Internet?
- How did cyber become global?
- How is cybersecurity global? What are the challenges associated with this?
- What are the side-effects of a global and open Internet?
- How do different countries address what citizens do on the Internet?
- How is Internet crime handled in the U.S.?
- How do different people view technology?
- How does technology impact social groups?
- Who owns a person's data?
- Who is responsible for cybersecurity?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
8.1.2 LO: Students will explain how the idea of the open internet led us to new innovations that impact our daily lives and our security.	• Computer, lecture slides, projector, graphic organizers, access to Internet • "What did we do before the Internet again?" *SEO for Breakfast*, 22 July 2018, https://www.seoforbreakfast.com/what-did-	• Have students answer the following questions: How did people buy things? How did people communicate? How did people find out what was happening in the world? • Have students map the following things to their modern equivalent. A library, a shopping center, a movie theatre, a book store, etc. • Encourage students to make up their own equivalent. Use the "What did we do before the Internet again?" image (linked left) for reference.

	we-do-before-the-internet/	
8.1.2a EK: The Internet provides global connectivity and is not structured around national boundaries.	• "How the Internet Was Invented | The History of the Internet, Part 1." *YouTube*, uploaded by SciShow, 1 Mar 2017, https://www.youtube.com/watch?v=1UStbvRnwmQ&feature=emb_logo	• Explain to students that the Internet started with a handful of research facilities on the west coast. Ask them how far the Internet reaches today. How did this happen? • Have students watch the video to see if their answers are correct.
8.1.2 LO: Students will explain how the idea of the open internet led us to new innovations that impact our daily lives and our security.	• *Internet Archive: Wayback Machine*. Internet Archive, https://archive.org/web/ • Tucker, Catlin. "Internet Archive: Go Back in Time with the Wayback Machine." *CatlinTucker.com*, 7 Jan 2019, https://catlintucker.com/2019/01/internet-archive-go-back-in-time-with-the-wayback-machine/	• Have students list ways the Internet has changed. Show them the Wayback Machine. • As described on the site linked on the left, have students research how the Internet has changed. Try to find the date of when a site was defaced. Have them look at the site before the defacement, the day it took place, and the days after. Have them look for news articles about the attack to examine the impact on the site and its users.
8.2 EU: Cybersecurity is global, transcending traditional	• "Top 20 Countries in Internet Users." *Internet*	• Using the Internet World Stats site, have students explore the current state of the Internet.

boundaries, and is always evolving.	*World Stats*, 30 June 2019, https://www.internetworldstats.com/top20.htm • "Individuals using the Internet (% of population)." *The World Bank*, https://data.worldbank.org/indicator/it.net.user.zs?end=2018&start=1960&view=chart	• Using the World Bank site linked to the left, have students check on the different types of graphs (line, bar, and map) to analyze Internet growth over the years. This could be done for individual countries, by decade, or by subscription type (cellular, telephone, broadband, etc.)
8.2.1c EK: Past and current laws are insufficient to assign blame for taking action that make our systems more vulnerable or to punish an entity for cyber crimes. 8.2.1a EK: Nation states have various approaches to sovereignty, investment and deterrence regarding cyber technology. 8.2.2a EK: Nation states have various approaches to civil rights and privacy regarding cyber technology.	• "Top 20 Countries Found to Have the Most Cybercrime." *EnigmaSoft*, https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ • Morgan, Steve. "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics." *Cybercrime Magazine*, 6 Feb 2019, https://cybersecurityventures.com/cybersecurity-almanac-2019/	• Ask students if Internet crime follows national boundaries. Have students examine the two sites to see how nations are impacted by cybercrime. • Ask students why some nations care about cybersecurity more than others. • Have them use the Global Cybersecurity Index linked on the left to see how different nations rank in their efforts.

8.2.1g EK: Cultural perceptions and priorities of security may differ between countries affecting how and which security measures are implemented.	• "Global Cybersecurity Index (GCI) 2018." *International Telecommunication Union (ITU)*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf	
8.2.1b EK: Cybersecurity is impacted by the state of a political alliance between nation states. 1.1.1d EK: Different communities and societies have different foundational social goals and values that impact their behaviors concerning technology.	• "Joint US - UK statement on malicious cyber activity carried out by Russian government." *National Cyber Security Centre (NCSC)*, 15 April 2018, https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government	• Discus this point, providing students with the example of the how the US and UK issued a joint statement regarding Russia in 2018. See link to the left for more information.
8.2.2c EK: When a government provides cybersecurity it can often lead to the reduction of privacy. 8.2.1a EK: Nation states have various approaches to sovereignty, investment and	• Pattison, Sandra. "Internet Censorship 2020: Find Out Where Repression Reigns." *Cloudwards.net*, 12 June 2020, https://www.cloudwards.net/internet-censorship/	• The site cloudwards.net (see left) offers a great deal of information on this point. This would be a good research opportunity for students. They could research by restriction or by assigned country. • This is a good place to discuss how the FBI investigates cybercrime in the United States. The FBI's IC3 site, linked to the left, offers various flyers and brochures about their efforts. It also includes statistics about victims, including

deterrence regarding cyber technology. 8.2.2a EK: Nation states have various approaches to civil rights and privacy regarding cyber technology. 1.1.1d EK: Different communities and societies have different foundational social goals and values that impact their behaviors concerning technology.	• *Federal Bureau of Investigation Internet Crime Complaint Center (IC3)*. Federal Bureau of Investigation, https://www.ic3.gov/complaint/default.aspx/.	number and dollars lost per age group. These statistics are helpful in exploring how different groups vary in their behaviors concerning technology.
1.1.1a: Societies are groups of individuals characterized by common interests/values that are perpetuated by persistent social interaction. 1.1 EU: Social goals reflect the foundational values held by society; these core societal values are reflected in cybersecurity choices. 1.1.1d EK: Different communities and societies have different foundational social goals and values that impact their behaviors concerning technology.	• "Cybersecurity and Human Rights." *PublicKnowledge.org*, https://www.publicknowledge.org/cybersecurity-and-human-rights/ • "The State of Cybersecurity in Latin America." *Trend Labs Security Intelligence Blog*, Trend Micro, 3 May 2013, https://blog.trendmicro.com/trendlabs-security-intelligence/the-state-of-cybersecurity-in-latin-america/	• Both Latin American and Nigerian attitudes about cybercrime are different than our society. The links on the left touch on these differences. Use a Venn diagram to help students illustrate how the attitudes vary. • Another avenue of investigation is how technology has impacted individuals with disabilities. • Students should also discuss the impact of technology and cybersecurity on politics, business, socialization, productivity, and privacy.

8.2.1g EK: Cultural perceptions and priorities of security may differ between countries affecting how and which security measures are implemented.	• "Letter from Africa: Why Nigeria's internet scammers are 'role models." *BBC.com*, 23 Sept 2019, https://www.bbc.com/news/world-africa-49759392 • "Mothers of 'Yahoo Boys' Now Forming Association." *Sahara Reporters*, 31 Oct 2019, http://saharareporters.com/2019/10/31/just-mothers-%E2%80%98yahoo-boys%E2%80%99-now-forming-association-%E2%80%93magu	
8.2.2 LO: Students will analyze how privacy concerns vary greatly in regards to societies, age, and socio-economic status. 1.1.1 LO: Students will analyze online and offline behaviors in societies, i.e., themselves, peers, families, communities, and	• "Digital Knowledge Quiz." Pew Research Center, *pewresearch.org*, https://www.pewresearch.org/internet/quiz/digital-knowledge-quiz/ • Birdsong, Toni. "15 Easy, Effective Ways to Start Winning Back Your Online	• Have students take the digital knowledge quiz linked on the left. When finished, have students compare their score with other Americans who took the quiz. • Have students make a community service poster discussing various ways to protect their privacy. The linked McAfee article is a good resource for this activity. • Poll students about their Facebook use. Show them the Facebook graphic linked on the left.

countries, and deduce the values that govern these behaviors.	Privacy." *McAfee.com*, 12 Oct 2019, https://securingtomorrow.mcafee.com/consumer/family-safety/15-easy-effective-ways-to-start-winning-back-your-online-privacy/ • "Since 2012, use of Facebook has grown fastest among older generations." Pew Research Center, *PewResearch.org*, 6 Sept 2019, https://www.pewresearch.org/fact-tank/2019/09/09/us-generations-technology-use/ft_19-09-03_digitaldividegenerations_2/ • Vogels, Emily A. "Millennials stand out for their technology use, but older generations also embrace digital life." Pew Research Institute,	• Next, have them poll people from each generation listed regarding their use of Facebook, a smartphone, a tablet, and use of social media to see if their research matches the ones linked on the left.

	PewResearch.org, 9 Sept 2019, https://www.pewresearch.org/fact-tank/2019/09/09/us-generations-technology-use/	
1.1.1c EK: Values concerning how to engage in cyber technologies can and do compete during the creative process of designing the technology and its adoption. 1.1.1b EK: Cybersecurity ethics is an expression of values by the designers and users. 8.2.1e EK: Depending on the values of the entity, some will invest in research and development, while others invest in reverse engineering the work of others. 8.2.1d EK: To ensure the safety of a nation's critical infrastructure both public and private sectors are responsible for cybersecurity.		• Discuss 1.1.1b EK and 1.1.1c EK with students. Explain that each person has two types of data (public and private). Companies often demand individuals divulge a lot of their private data. Should companies have to protect this data? Have students read an app usage agreement to see how much private data the app has access to. • Digital/voice assistants like Google Home and Alexa are excellent products to use to study these points. • Discuss the differences between R&D and reverse engineering. What are the pros and cons of both? In what situations is reverse engineering illegal. • Explore how ransomware has hit businesses, hospitals, schools, and cities. How were people impacted?
8.2.1f EK: Citizens in cyber space can more readily form ideological communities which is impacting		• Ask students if they have connections online with people they have never met. Have they ever watched a video made

what it means to be a nation state. 8.2.2b EK: The combination of increasing power of new technology and the declining clarity and agreement on cybersecurity and privacy gives rise to problems concerning law, policy and ethics. 8.2.2c EK: When a government provides cybersecurity it can often lead to the reduction of privacy.		a someone in a different country? Note the benefits of global connectivity (information sharing, communication, bank and shopping, selling and making money, IoT devices, sharing resources/cloud computing, entertainment, etc.). Does this impact how we see the world. • This connectivity also brings about challenges (bullying, crime, addiction/time loss, spam, health and mental issues, loss of national identity, loss of privacy, etc.). Have students list the pros and cons. • Discuss the deep web and dark web. How does the dark web impact law and ethics?
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.		• Discuss a career related to these topics (digital forensics, privacy officer, or compliance manager)

UNIT 5: Cybersecurity Law

Estimated Time in Hours: 6

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
4 Data Security 1 Ethics 8 Implications	4.2	- Research the adoption of a technology and find related legislation regarding the technology. - Compare and contrast iconic cybersecurity legislation. - Examine types of cryptography that can and cannot be exported.

Guiding Questions:

- What are the differences between policy and law?
- What are examples of each?
- What are the types of cybersecurity law?
- Why does legislation have a hard time keeping up with technology?
- What are other challenges in creating cyber law?
- What is Personally Identifiable Information?
- What are some examples of state, national, and international legislation?
- Is hacking legal?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
4.2.1 LO: Students will compare and contrast data protection legislation, policies, and procedures that have been or are being introduced all over the world to protect personal data.	• Computer, lecture slides, projector, graphic organizers, access to Internet	• Show students pictures of different crimes being committed. Ask the students to identify what is happening in the pictures. Ask what they have in common and what the punishment should be for each crime. Ask students if a computer could be used to aid/detect each of the crimes. • Explain the differences between policy and law. Schools may have policies, but they do not have laws. This distinction is important later.

4.2.1g: An Acceptable Use Policy is a set of rules applied by the owner, creator or administrator of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used.	• "Acceptable use policies." *YouTube*, uploaded by DrPete Technology Experts, 3 Mar 2015, https://www.youtube.com/watch?v=t78LXufrqnA • "Sample Acceptable Usage Policy." Get Safe Online, *GetSafeOnline.org*, https://www.getsafeonline.org/themes/site_themes/getsafeonline/download_centre/Sample_Acceptable_Usage_Policy.pdf	• Explain that one example of a policy is an acceptable use policy. The video linked on the left explains what this is. • Have students find an acceptable use policy, summarize its contents, and compare it to the example linked on the left.
Click or tap here to enter text.		• Discuss the differences between civil and criminal law. • Have students list ways a computer can be used in civil law offenses (breach of contract, property damage, slander) and criminal law (homicide, possession of a controlled substance, data theft). • Discuss the ways computers can be used in crime: -Computer-assisted -Computer-targeted -Computer as incidental

1.3.3b EK: Technology moves faster than laws can be created to govern it	• "Over 50 Years of Moore's Law." Intel, *Intel.com*, https://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html • Desjardins, Jeff. "The Rising Speed of Technological Adoption." Visual Capitalist, *VisualCapitalist.com*, 14 Feb 2018, https://www.visualcapitalist.com/rising-speed-technological-adoption/ • Smiley, Lauren. "A Brutal Murder, a Wearable Witness, and an Unlikely Suspect." Wired Magazine, *Wired.com*, 17 Sept 2019, https://www.wired.com/story/telltale-heart-fitbit-murder/ • Whittaker, Zack. "Judge orders Amazon to turn over Echo recordings in	• Discuss Moore's law (not a law but a theory). The video on the left is a good way to introduce it. • Using the Visual Capitalist site, have students look at the rate technology has progressed. Assign each students an item off the list from the site (click on Add technology on the right side of the graph). Have students find the years the technology took from introduction to full adoption. Have them research laws regarding the technology and give a report. • Ask student why technology moves faster than laws can be created. Students could look for examples, such as cryptocurrency, Fitbit Data, or Amazon Echo data, to explore this topic. Two relevant articles are linked on the left. • Have students brainstorm why cybersecurity laws are slow to be created. There are articles on the left to help with this. • Also discuss scope of legislation and the need to not stifle development. • Discuss the difficulty of determining jurisdiction and prosecuting people and business committing crimes in the US who are based in other countries.

	double murder case." Tech Crunch, *TechCrunch.com*, 14 Nov 2018, https://techcrunch.com/2018/11/14/amazon-echo-recordings-judge-murder-case/ • Harris, Marci. "Here's what happens when tech outpaces government." Apolitical, *Apolitical.co*, 12 Sept 2019, https://apolitical.co/solution_article/heres-what-happens-when-tech-outpaces-government • Selk, Avi. "'There's so many different things!'; How technology baffled an elderly congress in 2018." The Washington Post, *WashingtonPost.com*, 2 Jan 2019, https://www.washingtonpost.com/lifestyle/style/theres-so-many-different-things-how-	

	technology-baffled-an-elderly-congress-in-2018/2019/01/02/f583f368-ffe0-11e8-83c0-b06139e540e5_story.html • Kaal, Wulf. "What Happens When Technology is Faster Than the Law?" The CLS Blue Sky Blog, *Columbia.edu*, 22 Sept 2016, http://clsbluesky.law.columbia.edu/2016/09/22/what-happens-when-technology-is-faster-than-the-law/	
4.2.1a EK: Policies can be introduced and enforced at the local, state, and national levels.		• Tie levels of policies and legislation to types of law.
4.2.1b EK: Laws are in place to protect the disclosure and misuse of financial, personal, and private information. 4.2.1f EK: CCPA (California Consumer Privacy Act) was signed into law in 2018. It is	• "Data Privacy Explained | Cybersecurity Insights #11." *YouTube*, uploaded by Absolute, 12 Feb 2019, https://www.youtube.com/watch?v=3YIPQrEWOeY	• Have students define privacy. Explain why privacy laws are needed. Have them predict areas where privacy laws would be needed (education, medical, finance, etc.) • Define Personally Identifiable Information (PII). Have students list examples. • Discuss CCPA and its implications (state level legislation.

intended to extend the privacy rights of the citizens of California. 4.2.1e EK: CFAA (Computer Fraud and Abuse Act) prohibits accessing a computer without authorization, or in excess of authorization. 4.2.1d EK: HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information. 4.2.1c: GDPR (General Data Protection Regulation) is a set of regulations designed to give citizens in the European Union more control over their personal data. 4.2.1 LO: Students will compare and contrast data protection legislation, policies, and procedures that have been or are being introduced all over the world to protect personal data.	• "Data Privacy Laws | Cybersecurity Insights #12." *YouTube*, uploaded by Absolute, 26 Feb 2019, https://www.youtube.com/watch?v=v9I8iDLFtgE	• Discuss FISMA (national level legislation). • Discuss CFAA (national level legislation). • Discuss HIPAA (national level legislation). • Discuss GDRP (international level legislation). • Activity: Have students create a poster or slideshow contrasting data protection legislation, policies, and procedures all over the world. This could be a summary of different countries, or a jigsaw activity, with each student doing an assigned country(ies). • Activity: Show the 2nd video linked left, and ask students to compare GDPR to CCPA (California's Law).

8.1.2c EK: Early government policies discouraged the use of encryption to build secure networks.	• "Information Security: Context and Introduction | Introduction to Cryptography; The Cryptography Dilemma." created by University of London, accessed via *coursera.org*, https://www.coursera.org/lecture/information-security-data/this-video-explains-why-control-of-cryptography-presents-society-with-a-dilemma-fbN2G • "Clipper Chip – Ethics in Computing." NC State University Computer Science Department, *NCSU.edu*, https://ethics.csc.ncsu.edu/style/privacy/encryption/clipper/ • Matthews, Tim. "The Clipper Chip: How Once Upon a Time the Government Wanted to Put a Backdoor in Your	• The Clipper Chip (MYK-78) is a good example of this. The video on the left discusses government control of cryptography. • Have students research technologies like the clipper chip and develop a list of pros and cons related to the technologies. Students should also discuss if the device is ethical. (there are 2 useful resources linked left which pertain to clipper chips.) An alternative would be to have students research China's censorship and view on encryption. The sources below would be helpful to these students. • Have students examine what types of cryptography can or cannot be exported (Encryption and Export Administration Regulations (EAR). The site linked on the left would help with this research.

	Phone." Exabeam, *Exabeam.com*, https://www.exabeam.com/information-security/clipper-chip/ • "FLOWCHART 1: ITEMS DESIGNED TO USE CRYPTOGRAPHY INCLUDING ITEMS NOT CONTROLLED UNDER CATEGORY 5, PART 2 OF THE EAR." Bureau of Industry and Security, U.S. Dept. of Commerce, *bis.doc.gov*, https://www.bis.doc.gov/index.php/documents/new-encryption/1654-flowchart1/file	
1.3.3 LO: Students will discuss how even when a cybersecurity practice is legal, it may not be ethical. 1.3.3a EK: The legal and ethical consequences of cybersecurity practices can be explored		• Have students discuss the ethical implications of the clipper chip. Although legal, is it ethical to use? • Introduce the concepts of white, gray, and red hat hacking. Stress that students need written permission from the involved parties to hack. • Discuss careers such as pen tester or cyber legal advisor.

through ethical versus malicious hacking. 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.		

UNIT 6: Data Security Concerns

Estimated Time in Hours: 6

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
4 Data Security 1 Ethics 8 Implications	4.1, 4.2	- Research common password recovery questions and determine how users can be tricked into supplying the information. - Research cyber warfare. - Research security clearances and the actions that can prohibit a person from qualifying for one. - Research what to do in the instance of identity theft. Using a VM, have students set up role-based and rule-based access controls. - Complete a hashing lab.

Guiding Questions:

- What is data confidentiality?
- What can be learned from someone's data, and how could a hacker use this information?
- What are the harms and benefits of data protection?
- What is cyber warfare?
- How is data managed and protected?
- How can people harm data?
- What is data security?
- What are different types of access control?
- What is origin integrity, and how do you prove it?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
4.1.1 LO: Students will analyze existing data security concerns and assess methods to overcome those concerns.	• Computer, lecture slides, projector, graphic organizers, access to Internet	• Ask students if they have ever experienced or known someone who experienced identity theft, an online account takeover, a direct cyber attack, or a breach. Have them compare their experience with the 2018 national

4.1.1g EK: Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.	• "ITRC Surveys, Studies and Whitepapers." Identity Theft Resource Center, *IDTheftCenter.org*, https://www.idtheftcenter.org/surveys-studys/ • "2018 End-of-Year Data Breach Report." Identity Theft Resource Center, *IDTheftCenter.org*, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf	results (identity theft = 15.23%, online account takeover = 22.84%, direct attack = 38.41%, and breach = 43.32%). Explain to students that every time that happens you are suffering an attack on confidentiality. • The site linked on the left has a lot of information for students to explore regarding identity theft. It also has an infographic (linked left) with fast facts you can discuss with the class. The PDF also highlights breaches by type, industry, and types of information exposed. • Have students look at the definition of data confidentiality and explain why it is important. • Discuss data types (regulated, PII, business/commercial, and collaborative data). Have students provide examples of each type.
4.1.1a EK: Data can reveal much about people, their thoughts, and lives; which makes personally identifiable information highly sensitive.	• Collins, J. Carlton. "Online security: The password-recovery questions you should be answering." Journal of Accountancy, *JournalOfAccountancy.com*, 1 Mar 2018, https://www.journalofaccountancy.com/issues/2018/mar/password-recovery-questions.html	• Ask students things an attacker can learn from someone's social media account, buying history, medical records, or browser history. • Tell students they have to come up with their own hacker names based on their favorite food and their mother's maiden name. Before they reveal their answers, ask them why this a bad idea. Ask if they have seen similar "games" on social media.

	• "Social Media Habits & You: Trend Analysis 2018." Identity Theft Resource Center, *IDTheftCenter.org*, https://www.idtheftcenter.org/wp-content/uploads/2018/10/ITRC_CyberScout_Social-Media-Habits-and-You-Survey_Trend-Analysis_2018_Web.pdf	• Have students research common password recovery questions (see link to left). How could attackers find this information? How could they leverage this knowledge? • How could attackers leverage social against a target? • Why would attackers target the social media accounts of people who work for organizations?
8.1.1c EK: Events in cyber warfare and cybercrime escalated the need for increased cybersecurity efforts 1.2.1 LO: Students will discuss how cybersecurity can significantly impact the quality of people's lives both positively and negatively. 1.2.1a EK: Examples in history demonstrate the harms and benefits of cybersecurity from multiple perspectives.	• Garrie, Daniel. "Defining cyberwarfare…in hopes of preventing it." *YouTube*, uploaded by TED-Ed, 20 Aug 2013, https://www.youtube.com/watch?v=ZVoDwtyvDJc&feature=emb_logo • *U.S. Army Cyber Command*. United States Army, https://www.arcyber.army.mil/ • "Fact Sheets." *U.S. Army Cyber Command*,	• Ask students if there is a "downside to cybersecurity." Possible answers are it being user centered (users are a weak link), it makes access slower, it can be expensive and become outdated quickly, the solutions can be used by criminals to hide from law enforcement. • Discuss the definition of cyber warfare. The video linked on the left may help with this. Have students research the role of the U.S. in cyberwarfare. Using the fact sheets linked on the left, ask students to create a presentation or poster on a cybersecurity-related topic.

	https://www.arcyber.army.mil/Info/Fact-Sheets/	
4.1.1b EK: Data can be used to help individuals, but it can also be exploited to harm individuals. 4.1.1c EK: Data must be protected in processing, transmitting and storage 4.2 EU: Data Security uses non-technical and technical controls and techniques to protect data that is being processed, transmitted and stored.	• "Developing and Using Security Classification Guides." Published by the Information Security Oversight Office (ISOO), updated Oct 2018, accessed via the National Archives, *archives.gov*, https://www.archives.gov/files/isoo/training/scg-handbook.pdf • Christensen, Michelle D. "Security Clearance Process: Answers to Frequently Asked Questions." Published by the Congressional Research Service, 7 Oct 2016, accessed via Federation of American Scientists, *fas.org*, https://fas.org/sgp/crs/secrecy/R43216.pdf	• Of course, the main weapon in cyberwarfare is data. Remind students of the three states of data (at rest, in motion, and in use). Point out to students that data must be protected in all three states. Have students map possible attack to the three data states. For example, Ransomware targets data at rest. • Discuss how data security utilizes technical and non-technical controls. One of these is through data classifications. Discuss data classifications used by businesses and government. How are they alike? How do they differ? • Using the document linked on the left, have students read about classification requirements and do the Three Little Pigs activity in the booklet. Next, have them research eligibility requirements for a security clearance and the investigation process.
4.1 EU: Data security deals with the integrity of the data, i.e., the protection from corruption or errors; the privacy of data; and	• Boadu, Edwin Okoampa and Armah, Gabriel Kofi. "Figure 1.1: Relationship Between Hospital	• Discuss access management with students (identification, authentication, authorization, and accounting). Provide the definition and examples.

data confidentiality, i.e., it being accessible to only those who have access privilege to it. 4.1.1d EK: The purpose of personal data protection is not to merely protect a person's data, but to protect the fundamental rights, freedoms, and welfare of persons who are related to that data 4.1.1 LO: Students will analyze existing data security concerns and assess methods to overcome those concerns.	Workers and Privilege." Role-Based Access Control (Rbac) Based in Hospital Management, *International Refereed Journal of Engineering and Science*, Vol. 3, Issue 9, Sept 2014, http://www.irjes.com/Papers/vol3-issue9/H395367.pdf	• Explain the purposes of data protections. Have students consider the emotional ramifications to users and the time lost in addition to the loss of privacy and financial impact. • Discuss data security strategies (physical, technical, and administrative). Provide examples of each. • Give students different scenarios and have them list physical, technical, and administrative controls to use in each scenario. • Discuss various access control models (MAC, DAC, RBAC, and RuBAC). Have students pick one and create a slideshow or poster with the characteristics and use case for each model. Figure 1.1 in the report linked to the left is an example of what the students could create. In a VM, have students set up a role-based and rule-based access control Example: Windows Live Family Safety
4.1.1f EK: Origin integrity means the original data is trustworthy, and its source is trusted to produce trustworthy data. 4.1.1e EK: Data integrity means only authorized changes are made only by authorized people. 8.1.1h EK: Cybersecurity events have led to the development of		• Ask students if they would like a $100 bill. What about a fake $100? Which is more valuable? Why? • Tie this to original integrity. It is important that we are able to trust data. Have students brainstorm examples where origin integrity would be important. Discuss how hashing helps prove origin integrity and how the access control models help create origin integrity. • Tie this unit to a cybersecurity career like cybersecurity architect.

various cybersecurity career paths and various needs in order to prepare people for these new types of jobs.		

UNIT 7: Principles of Software Design

Estimated Time in Hours: 5

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust	2.2, 2.3	- Practice recognizing and differentiating the principles using resources such as the GenCyber principles card game. - Practice minimization by installing a simple firewall and configuring its rules (a raspberry pi firewall example is given).

Guiding Questions:

- What are principles and how do they differ from rules?
- What is the difference between simplicity and minimization?
- What is the difference between domain separation and process isolation?
- What is the difference between resource encapsulation and information/data hiding?
- Why are fail-safe defaults important, especially in software design?
- Do these 11 principles guarantee security?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
2.2.1 LO: Students will describe the principle of simplicity, which is about ensuring that systems are easy to understand, maintain and test so as to be more secure.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Resource for GenCyber 10 Principles (note: does not cover all 11 principles presented here, but a great resource for the others):	• Introduce the 11 Principles using Saltzer and Schroeder's 1975 paper "The Protection of Information in Computer Systems" (note: originally 8, now expanded to 11). Note: the 11 Principles are introduced in this unit; however, they are expanded upon in future relevant units. • Show students common web home pages (i.e., Google, Yahoo). Ask them which one holds a more simplistic design and how it is easier to understand, maintain, and test.

	Hale, Ghandi, Morrison, and Rausch. "Introduction to Cybersecurity First Principles." *GitHub*, uploaded by mlhale, https://mlhale.github.io/nebraska-gencyber-modules/intro_to_first_principles/README/ • GenCyber Principles Card Game: "Game Instructions." Cyber Realm, *gencybercards.com*, https://gencybercards.com/instructions	
2.2.1a EK: Simple designs are easier to understand, maintain and test for security problems. 2.2.1b EK: Simplicity is also known as "Economy of Mechanism."	• Economy of Mechanism: "Engineering Maintainable Android Apps – Economy of Mechanism." *YouTube*, uploaded by intrigano, 31 Oct 2017, https://youtu.be/TNBSSIrKXnE	• Have students watch the YouTube video to define Economy of Mechanism and why it is needed. • Challenge students to answer why is could be a bad idea to include functions and features that aren't needed.

2.2.1cEK: A simple design incorporates a careful analysis of what is needed	• Guide on steps to simplify cybersecurity: Chiock, Mario. "8 Steps to Simplify Cybersecurity." *SecurityRountable.org*, 4 Apr 2019, https://www.securityroundtable.org/8-steps-to-simplify-cybersecurity/?doing_wp_cron=1589219255.4833331108093261718750	• Walk through the steps provided by the web source to demonstrate how to achieve simplicity.
2.2.2LO: Students will use the principle of abstraction to represent complicated concepts more simply and to allow solutions to be transferred to other contexts. 2.2.2a EK: Abstraction is reducing the complexity of an object down to its essentials in a way that is understandable.		• Task students with matching examples of abstraction with what they represent (e.g., a car instrument panel & the car's parts, an illustration of a person & a picture of them, a tablet & the code running on it).
2.2.2LO: Students will use the principle of abstraction to represent complicated concepts more simply and to allow	• Abstraction from binary numbers: Domas, Chris. "The 1s and 0s behind cyber warfare." *YouTube*,	• Show the YouTube video where Chris Domas uses abstraction to categorize binary data into a visual representation that can be interpreted quickly. Ask students to identify specific ways he uses abstraction.

solutions to be transferred to other contexts. 2.2.2b EK: Good and elegant design involves using abstraction.	uploaded by TED, 30 June 2014, https://youtu.be/cWpRxyqDgpM	• Frame abstraction as a way to represent complicated concepts more easily. Ask them what colors are often used for danger, or what shapes are often tied to ideas. Stress this importance for developing UI and GUI. • Assign students abstract nouns and have them come up with a graphic representation of them.
2.2.3 LO: Students will apply the principle of minimization by decreasing the number of ways in which attackers can exploit a program or device.	• Raspberry Pi activity [install a simple firewall (UFW) on the pi and configure rules to block traffic from specific IP addresses, ports, etc.]: "Securing your Raspberry Pi." *RaspberryPi.org*, https://www.raspberrypi.org/documentation/configuration/security.md	• Show examples of minimization which students can relate to: turning off Wi-Fi when not in use and disabling Bluetooth when not in use. This can be as simple as not leaving a car running when it is parked and not in use. • Students can practice minimization by installing a simple firewall (resource reference UFW for the Raspberry Pi) and making firewall rules. These can be tested with multiple pis.
2.2.3a EK: The attack surface of a software environment is the sum of the different points where an unauthorized user can try to enter data or to extract data from an environment.	• Attack surface: "The Threat Landcsape Attack Surface." *YouTube*, uploaded by Muhammad Farooq, 28 May 2019, https://youtu.be/gvkWKKbTkx8	• Show the YouTube video introducing attack surfaces. Use a viewing guide with the video and have students write down attack surface examples in the video and how minimization can remedy them.
2.2.3b EK: Minimizing the attack surface decreases the	• Minimize attack vectors on Android:	• Task students with exploring how to minimize the attack surface on their own phones.

opportunity to find an exploitable vulnerability in the system. 2.2.3d EK: Common mechanisms and access should be minimized. 2.2.3c EK: The human interface should be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.	Raphael, JP. "10 Android Settings that'll strengthen your security." Computerworld, *computerworld.com*, 20 Nov 2018, https://www.computerworld.com/article/3268079/android-security-settings.html • Minimize attack vectors on iOS: Whittaker, Zack. "Cybersecurity 101: Five settings to secure your iPhone or iPad." Tech Crunch, *TechCrunch.com*, 19 Feb 2019, https://techcrunch.com/2019/02/19/cybersecurity-101-guide-ios-12-privacy/	
2.3.1 LO: Students will give examples of the principle of domain separation, which allows for the enforcement of rules governing the entry and use of	• Introduce concept of domains: "Introduction to Domains." *YouTube*, uploaded by Eli the	• After introducing the domains, ask students to list examples of domains in real-life. Examples include residential vs commercial areas; sidewalks vs roadways; and restaurants with their own seating areas.

domains by entities outside the domain. 2.3.1a EK: A domain refers to a collection of data or instructions that warrant protection.	Computer Guy, 16 Feb 2011, https://youtu.be/ut_oLhMhJsYa (Show 2:48 – 10:55)	• Students can work together to brainstorm ways in which these domains can be protected.
2.3.1b EK: Communications between domains are allowed only as authorized.		• Explain the school's network as sets of domains. Students and teachers can both access the network, but likely with different restrictions. • Ask students if they are allowed to access the teacher/staff network and whether that would violate domain separation.
2.3.2 LO: Students will know that the principle of process isolation prevents tampering or interference from/by other processes. 2.3.2a EK: A process is a program running on a computer.		• Demo process isolation by opening Task Manager (Ctrl+Shift+Esc in Windows). Explain how each item in the processes tab is separated. • Ask students why it is important to isolate processes. What happens if a program crashes or freezes? Demo ending a process and discuss how it only affects the target process.
2.3.2a EK: A process is a program running on a computer. 2.3.2b EK: Each process has a region of the memory (address space), which only it can access. 2.3.2c EK: Processes have to use defined communications	• Process isolation demo: "Cyber security Process Isolation." *YouTube*, uploaded by Phyllis adkins, 26 July 2018, https://youtu.be/HrY9KaCfKDs	• Explain why processes must be separated. Demo the example from the video if resources are available. • Have students research the terms namespace, resource control, and process isolation technologies. These are used by the operating system to achieve process isolation.

mediated by the operating system to communicate with other processes.		• Other examples include Google Chrome separating processes by tab, allowing one tab to crash without harming the others.
2.3.3b EK: Encapsulation allows access or manipulation of the class data in only the ways the designer intended	phpdevster. "Encapsulation. This is the easier of the two concepts to understand…" [Comment on the online forum post *ELI 5: Abstraction vs Encapsulation?*], Reddit, *Reddit.com*, https://www.reddit.com/r/javascript/comments/3shetz/eli5_abstraction_vs_encapsulation/	• Explain the resource part of resource encapsulation first. Students should be familiar with computer components by this point. Ask them to list the resources of a computer. This principle is often difficult for students to understand. Use a simplified example as explained on the website provided: "Consider another real-world example: your house. Your house is an encapsulation of how people go in and out of it. You must enter and leave only through doorways. People can't just randomly enter from any side or direction. The equivalent of a non-encapsulated house would be a house that has no walls, and a roof supported only by a few pillars." Example: medicine is encapsulated inside a gelatin capsule.
2.3.3a EK: Examples of resources are the memory, disk drive, network bandwidth, battery power, and a monitor. It can also be system objects such as shared memory or a linked list data structure. 2.3.3 LO: Students will explain the importance of encapsulating resources, i.e., creating well-defined interfaces around	• Encapsulation explanation: "What is Encapsulation." *YouTube*, uploaded by OOP Channel, 27 Mar 2017, https://youtu.be/bSpPwVFEbO8	• Use a viewing guide to review encapsulation examples and definition from the linked YouTube video.

resources to set rules for how the resources should interact.		
2.3.4c EK: Granting only those privileges necessary for a user to accomplish assigned duties improves accountability and limits accidental misuse. 2.3.4a EK: A privilege is a right for the user to act on managed computer resources.	• Least privilege example: "Least Privilege vs. Shared Accounts." *YouTube*, uploaded by Centrify, 23 Apr 2015, https://youtu.be/GXQsD5-noPM • Access Control List (ACL) manipulation in Linux: Newell, Glen. "An introduction to Linux Access Control Lists (ACLs)." Red Hat, *RedHat.com*, 6 Feb 2020, https://www.redhat.com/sysadmin/linux-access-control-lists	• Use a viewing guide with the linked YouTube video. Students should be able to describe how least privilege was used in the video's example. • Ask students how least privilege improves accountability and limits accidental misuse in this scenario and others.
2.3.4b EK: Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.		• Challenge students by tasking them to research the various types of access control (mandatory, role-based, etc.). They can research the types of access control individually and collaboratively create a poster with descriptive terms of each access control type. • Have students practice least privilege by manipulating Access Control Lists (ACL) in Windows and Linux (linked resource).

2.3.4 LO: Students will explore the principle of least privilege, which is about differentiating among types of access control (mandatory, role-based, discretionary, and rule-based access controls) and analyzing which to use for selective restriction of access to a place or other resource.		
2.3.5 LO: Students will break down how the principle of layering is a strategy for slowing down an attack because the attacker has to conquer each layer before moving on to the next. 2.3.5a EK: A layer is a separate level that must be conquered by an attacker to breach a system.	• Layering (defense in depth) introduction: "Network Security | Defense in Depth." *YouTube*, uploaded by Network Direction, 9 July 2019, https://youtu.be/IiWFMIgKaqQ	• Show the students a simple graphic of layering, such as a castle or fort. Have the students list the individual layers used. Does each layer make it more difficult for an adversary to achieve their goals? What happens if one layer fails? • Alternatively, use a viewing guide with the video to assess the students similarly.
2.3.5b EK: Multiple independent layers require integration and independent management to get the full benefits of layered protection.		• Introduce the types of layering in an effective defense: physical, technical, and administrative. These will be covered multiple times in future sections, but it is important for students to distinguish these categories early.
2.3.6 LO: Students will know that the principle of data hiding is about allowing only necessary aspects of a data structure or a	• Information hiding introduction:	• Make students explain the difference between encapsulation and information hiding.

record to be observed or accessed. 2.3.6a EK: Data hiding can help prevent users/programmers/processes from updating/changing data in invalid ways or by mistake.	"Information Hiding." *YouTube*, uploaded by Udacity, 23 Feb 2015, https://youtu.be/zaqiMBoGFO4	• Ask students to research ways information hiding is achieved in computers.
2.3.7a EK: The principle of modularity says that individual components are capable of executing a unique part of the desired functionality and is achieved through system design. Because of this modular design, security upgrades can happen in one component without having to overhaul the entire system. 2.3.7b EK: A system's components may be separated and recombined.	• Modularity in product design: "WHY MODULAR PROJECT DEISGN?" *YouTube*, uploaded by Modular Management, 18 July 2017, https://youtu.be/p6liu6Ro1bE	• Ask students how computers employ modularity. If a hard drive fails, can another replace it? If a second monitor is desired, can it be added? • Have students research systems (technical and non-technical) which employ modular design. Is modularity a benefit in these cases?
2.3.8 LO: Students will define the principle of fail-safe defaults, which restricts how privileges are initialized when a subject or object is created. 2.3.8a EK: When something does not work or the system fails, the	• The beginning of this video shows a couple good examples of fail-safe not involving computers (lawn push mowers, automatic shopping mart doors):	• Discuss how the ultimate goal of a fail-safe is to protect the assets. With fail-safe, security will beat availability. • Present the students with scenarios and have them judge whether it should be or is fail-safe. Should functionality be sacrificed for security?

system must return to a secure state	"Nuclear Reactor Fail-safe." *YouTube*, uploaded by Randy Dobson, 2 July 2017, https://youtu.be/y_kePiYWl4w	
2.3.8b EK: A secure state is a condition when no subject can access any object in an unauthorized manner 2.3.8c EK: Turning off permission causes a security problem. Please read the following comment from the creator about this EK.		• Explain the broader goal is that a system should come with secure initial settings and should reset to a secure state if rebooted/restarted/reset. This could be applied to the software you install on your computer or the device you connect to your home network. Note: the concept of fail-safe in computers is different than fail-safe in physical security. In physical security, fail-secure is the closer definition to this principle.
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 instructor.

UNIT 8: Cybersecurity Business Economics

Estimated Time in Hours: 8

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
8 Implications 1 Ethics	8.3, 1.3	- Examine terms of service agreements for various companies to create a wall of fame and wall of shame. - Research the reactions of businesses after breaches to determine the level of transparency.

Guiding Questions:

- If you are buying a piece of technology, how do you decide what to purchase? What factors do you consider?
- Do consumers view security as a selling feature?
- Why do companies struggle with cybersecurity?
- How should companies address cybersecurity?
- What happens if a company does not invest in cybersecurity?
- Why do businesses get cybersecurity wrong?
- Are businesses prepared for cyber attacks?
- What do businesses stand to lose for being unprepared?
- How does supply chain impact cybersecurity?
- What do consumers need from businesses regarding cybersecurity?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
8.3.3 LO: Students will describe how economics shape the decisions of consumers. 8.3.3a EK: Consumers are often driven by new functionality which is tangible while the security features of the product	• Computer, lecture slides, projector, graphic organizers, access to Internet "Intro to Economics: Crash Course Econ #1." *YouTube*, uploaded by CrashCourse, 8 July 2015,	• Ask students what factors into their decisions when making a technology-related purchase. What features are important to them? You might need to use a specific piece of technology as an example to narrow the scope (television, cell phone, tablet, etc.). Is security ever a consideration? What about for the average consumers; do they consider security?

may only be understood or appreciated when the security fails. 8.3.1a EK: Economic value typically measures gains achieved, not losses avoided.	https://www.youtube.com/watch?time_continue=110&v=3ez10ADR_gM&feature=emb_logo	• Depending on the students' background, they may need the video linked to the left to better understand economics. Why is economic value typically measured in gain achieved instead of losses avoided? Ask students for examples.
8.3 EU: Measuring the economic value of cybersecurity is often an indirect process that relies on risk management trade- offs rather than direct benefits.	• Mňuková, Kateřina. "The Boat Game. Fun way how to teach your team start caring about the risks." Medium, *Medium.com*, 27 Mar 2018, https://medium.com/@katerina_mnuk/boat-game-62916dadb70 • Whiting, Jim. "Titanic–Not Enough Lifeboats." iNK Think Tank, *NonfictionMinute.org*, 2 May 2020, https://www.nonfictionminute.org/the-nonfiction-minute/titanic-not-enough-lifeboats • Javaherdashti, Reza and Akvan, Farzaneh. "Figure 3: Risk Assessment Matrix." On the Link Between Future Studies and Necessity of	• Ask students how much a company should spend on cybersecurity? How much is enough? • Use the game linked on the left to introduce the idea of risk managements. This game could be adjusted to fit the scenario of the Titanic using the information linked on the left.

	Including Corrosion in a 'Desired Future' Scenario: Presenting a Model, *International Journal of Engineering Technologies and Management Research*,. 24. 1-8., 2015, accessed via Research Gate, *researchgate.net*, https://www.researchgate.net/figure/An-example-of-a-Risk-Assessment-Matrix_fig3_283150764	
8.3.3d EK: Ill-informed consumers and businesses are prone to underinvest or invest in wrong solutions if they do not possess an accurate understanding of threats and defenses. 8.3.1 LO: Students will explain how misaligned incentives encourage businesses to under invest in cybersecurity.		• Ask students what happens if companies do not invest in cybersecurity? Have students investigates examples of this. • Explain to students that, for businesses, cyber attacks are difficult to predict, limited by bureaucracy, difficult to implement, and difficult to evaluate. Attacks are hard to investigate and prosecute. However, for the attacker, attacks are easy to produce, cheap to launch, easy to adapt, hard to investigate, and hard to prosecute.
8.3.2 LO: Students will explain how economic forces influence the cybersecurity choices made by service providers and service designers.	• Carfagno, Don. "How Much Should Your Company Invest in Cybersecurity?" CyberShark,	• Have students research the impact of a cyberattack on small businesses. Suggest examples similar to the ones on the left.

8.3.1b EK: The lack of cybersecurity can cause substantial economic losses; including the compromise of sensitive data, the modification of critical data, the improper behavior of a system, or the unavailability of a system. 8.3.1d EK: When misaligned incentives arise the party making the security–efficiency trade-off is not the one who loses out when attacks occur. 8.3.1c EK: The lack of cybersecurity can result in major financial and reputational loss, but this loss only occurs after a successful attack. 8.3.1d EK: Even in the event of a successful attack, the loss may or may not have lasting direct economic impact on the provider of the service.	*BlackStratus.com*, 4 Nov 2018, https://www.blackstratus.com/how-much-should-your-company-invest-in-cybersecurity/ • Miller, Gary. "60% of small companies that suffer a cyber attack are out of business within six months." The Denver Post. *DenverPost.com*, updated 24 March 2017, https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/ • "Cyber attacks – impacts and risk management for organisations." *YouTube*, uploaded by Dentons, 26 Sept 2017, https://www.youtube.com/watch?v=gySzp3RrXjo&feature=emb_logo	• Ask students what business have to lose if they do not invest in cybersecurity. The video linked on the left can help with this. • Discuss who else suffers when businesses are not prepared for an attack.
8.3.2c EK: Cybersecurity risks occur when outsourcing the production or maintenance of	• Wouk, Kris. "Where are iPhones Made?"	• Explain to students that businesses also have to consider their supply chain. Have students research all the

technology to third party sources that may have different security practices.	MakeUseOf, *MakeUseOf.com*, 28 May 2019, https://www.makeuseof.com/tag/where-are-iphones-made/ • Greenberg, Andy. "Supply Chain Hackers Snuck Malware Into Videogams." Wired Magazine, *Wired.com*, 23 Apr 2019, https://www.wired.com/story/supply-chain-hackers-videogames-asus-ccleaner/	different countries where iPhones are made. Are all these countries trusted by the U.S.? Why would this be a concern for the U.S. military? Let students know that supply chain is not just a military concern. Have them read about the Asus supply chain breach linked to the left.
8.3.2d EK: Whenever security depends on the weakest link in the global supply chain, firms do not prioritize in investing in security when they know that other players will not invest, leaving them vulnerable in any case.	• "Software supply chain attacks explained." *YouTube*, uploaded by Windows, 10 Sept 2018, https://www.youtube.com/watch?v=uXm2XNSavwo	• Have students watch the video link on the left. How is supply chain security dependent on the weakest link?
8.3.3b EK: In order to fully participate in today's economy, consumers must give away their data and agree to a company's terms that may conflict with their values.	• *Terms of Service; Didn't Read*, https://tosdr.org/ • "How to Monetize Your Data." Lotame, *lotame.com*, 13 Jan 2020,	• Since not all companies have a consumer's best interest in mind, consumers need to consider how a company will use their information. This is often spelled out in a terms of service agreement. Have students pick a product or application they use and find the terms of service agreement. They should read the agreement, making

8.3.3c EK: Consumers are often unaware of the value of their information that they exchange for an incentive from a company that uses their data for monetary purposes.	https://www.lotame.com/how-to-monetize-your-data/	note of how the company handles their privacy. Next, students should visit the site on the left and see how the site rates companies (just scroll down upon getting to the site). Based on these criteria, what score would their choice have. • Ask students if it is okay for a free service (like Google for Facebook) to sell your browsing history to advertisers. Have students look at it from a business's perspective by reading the article linked to the left.
1.3.1 LO: Students will explore the tensions that exist between transparency, autonomy, resilience and security. 1.3.1a EK: Transparency in cybersecurity is important for trustworthiness but can come at a risk to security. 1.3.1b EK: Autonomy is the idea that every entity is in control of their own thoughts and actions. 1.3.1c: EK Resilience is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.	• "Timehop Security Incident, July 4th, 2018." *Timehop.com*, updated 11 July 2018, https://www.timehop.com/security/ • "Four 9s vs Five 9s: What's the Real Cost of the Difference?" Intelligent Fiber Network, *IntelligentFiber.com*, https://www.intelligentfiber.com/four-9s-vs-five-9s-whats-the-real-cost-of-the-difference/	• Have students define the terms *transparency, autonomy, resilience* and *security*. How do these terms compete? Why are they important to consumers? • Have students go to the linked information on the left and discuss this press release with students. How does it demonstrate transparency? • Discuss autonomy and resilience with students. Ask students what percentage of the time they expect a service (like Google) to be up and running? How long can a service be down before it is considered unreliable? Discuss the 5 nines of uptime. The site linked to the left can help with this concept.

1.3.1d EK: Security is freedom from potential harm or other unwanted coercive change caused by others. 1.3 EU: Cybersecurity practices are highly complex and variable causing tensions between what the ethical duties are, to whom the ethical concern should be considered, and whose interests should be invested in protecting. 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.		• Discuss the meaning of "security is freedom." What is the difference between security and privacy? • Have students debate why cybersecurity issues are complex and why tensions exist. See example below. Example: Let's say there is a small business suffers a data breach. It is small, and only a few people were impacted. Should the company make the breach public? - If they do, the company could go out of business and employees would lose their jobs. - If they don't similar businesses might suffer a similar breach. • Have students explore a career, such as executive cyber leadership.

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.

UNIT 10: Cryptography

Estimated Time in Hours: 8

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
4 Data Security 8 Implications	4.3, 8.1	- Practice various forms of symmetric cryptography using GUI interfaces and command line tools. - Paper-craft physical historical ciphers to reinforce concepts. - Decode Enigma machine messages in realistic scenarios.

Guiding Questions:

- How is information protected on the Internet?
- What is the process to turn plaintext into ciphertext?
- What is needed to decrypt a message?
- What are some common attacks against ciphers?
- What is the primary difference between symmetric and asymmetric cryptography?
- What are the two basic uses for asymmetric cryptography?
- How can you check Certificate Authorities used for web browsing?
- How has cryptography played a major role in warfare?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
4.3.1g EK: The primary goal of cryptography is to keep enciphered information secret.	• Computer, lecture slides, projector, graphic organizers, access to Internet	• Ask students if they believe the Internet (social media, banking, gaming, e-commerce) is important to protect and whether they think it's safe. Ask how they believe things connected to the Internet are secured.
4.3.1 LO: Students will define cryptography and explain how it is used in data security.		• Introduce and define cryptography. You may give examples of secret writing or ask them to brainstorm how they would send a secret message.

4.3.1a EK: Cryptography comes from two Greek words meaning "secret writing" and is the art and science of concealing meaning.		• Explain the difference between encryption and decryption. Emphasize the importance of encrypting information so adversaries cannot access it. • Affirm the question posed before: The Internet is protected by cryptography. • Explain how cryptography was important before the Internet and give examples of historical methods of encryption and their purpose.
4.3.1f EK: Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result.		• Explain the difference between plaintext and ciphertext. Use a before-and-after example from historical cryptography to show the difference. "You can plainly read the plaintext." • Introduce the term key as a requirement to change between plaintext and ciphertext.
4.3.1d EK: Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.		• Focus on the definition of encryption. Use a historical encryption example to the process of encryption.
4.3.1e EK: Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.	• "Cryptology STEM workshop 60-90 Mins." University of Colorado Colorado Springs Center for STEM Education, *UCCS.edu*,	• Emphasize the definition of decryption. Use the same historical example to show the process in reverse. • Task the students with building a historical cipher (e.g., scytale) and using it to encrypt and decrypt messages. Discuss any vulnerabilities in the chosen cipher.

	https://www.uccs.edu/Documents/pipes/cryptology-cdio.pdf • *AES Crypt*, https://www.aescrypt.com/ • *OpenPGP*, https://www.openpgp.org/	• Digital cryptography can be practiced on Windows or Linux machines using the provided AESCrypt and GPG resources. • Review the various cryptography terms they have learned so far.
4.3.2 LO: Students will practice symmetric cryptosystems to send a message and explain how they work.	• Sweigart, Al. "Cracking Codes with Python– Chapter 1: Making Paper Cryptography Tools." Invent with Python, *InventwithPython.com*, https://inventwithpython.com/hacking/chapter1.html • Sweigart, Al. "Cipherwheel." Invent with Python, *InventwithPython.com*, https://inventwithpython.com/cipherwheel/ • "Cryptography Worksheets– Worksheet 1: The Caesar Cipher." CS Unplugged for Middle	• Task students with practicing symmetric cryptography algorithms (e.g., Caesar cipher). Depending on skill level, they can create physical representations of the cipher, practice using online tools, or develop software to simulate the cipher. • Provide independent practice with cryptography using the provided csunplugged resource.

	Schools, Colorado School of Mines, *Mines.edu*, http://csunplugged.mines.edu/Activities/Cryptography/CryptographyWorksheets.pdf	
4.3.1b EK: Cryptanalysis is the breaking of codes. 4.3.2e: A shift cipher is susceptible to a statistical ciphertext-only attack.	• "Lesson Plans & Activities– Frequency Analysis Code Cracker." Spy Museum, *SpyMuseum.org*, https://spy-museum.s3.amazonaws.com/files/resources/code-cracker.pdf • "Caesar Cipher." dCode, *dcode.fr/en*, www.dcode.fr/caesar-cipher	• Provide examples of cryptanalysis. • Task students with cracking frequency analysis ciphers and exploring the feasibility of brute-force attacks. Tie this to the identifying strong vs weak ciphers.
4.3.1c EK: Cryptographic algorithms, also known as ciphers, are mathematical functions used in the process of encryption and decryption.		• Recap ciphers covered so far and introduce new ones. • Ask students why we have so many ciphers and how they think they have evolved over time.
4.3.2a EK: There are two basic types of symmetric ciphers: Transposition ciphers that diffuse		• Explain the difference between transposition and substitution ciphers

the data in the plaintext and substitution ciphers that replace the data in the plaintext. 4.3.2b EK: In transposition ciphers the letters are not changed they are rearranged. The set of encryption functions E is simply the set of permutations of m, and the set of decryption functions D is the set of inverse permutations. 4.3.2c EK: Anagramming is a way to attack a transposition cipher. It uses tables of n-gram frequencies to identify common n-grams.		• Show simple examples of how transposition would encrypt plaintext. Use historical ciphers as examples and ask students to identify whether they are transposition. • Discuss weaknesses of transposition ciphers. • Highlight the anagram attack and how it works. Have students spot commonly used anagrams in English.
4.3.2d EK: A substitution cipher changes characters in the plaintext to produce the ciphertext.		• Show simple examples of how substitution would encrypt plaintext. Ask students to identify historical ciphers that are substitution. • Ask what kind of techniques substitution ciphers are vulnerable to.
4.3.1h EK: Symmetric encryption is a method of encryption involving one key for encryption and decryption.		• Emphasize how symmetric cryptography must use the same key and list the ciphers you've covered so far that are symmetric. • Ask students what would happen if a symmetric cipher used a different key to decrypt.

4.3.1i EK: Public key encryption, which is asymmetric, is an encryption method that is widely used because of the enhanced security associated with its use.	• "Asymmetric encryption – Simply explained." *YouTube*, uploaded by Simply Explained, 30 Oct 2017, https://www.youtube.com/watch?v=AQDCe585Lnc&feature=emb_logo • "Prime Numbers & Public Key Cryptography." *YouTube*, uploaded by Simon Pampena, 2 Nov 2011, https://www.youtube.com/watch?v=56fa8Jz-FQQ	• Contrast asymmetric cryptography to symmetric. Emphasize how asymmetric means "not the same." • Show the video on asymmetric encryption and ask students review questions, including why two keys might be advantageous in some situations. • If the class is keen on how it is so secure, show the video on prime numbers in asymmetric cryptography. Consider creating a viewing guide to review how prime numbers are beneficial.
4.3.3 LO: Students will employ public key (asymmetric) encryption and explain how it works. 4.3.3b EK: Public key encryption uses a key pair - a private key known only to the entity and a cryptographically linked public key that can be shared with anyone.	• "Bitcoin: How Cryptocurrencies Work." *YouTube*, uploaded by SciShow, 21 Dec 2016, https://www.youtube.com/watch?v=kubGCSj5y3k	• Contrast private and public keys. Be sure students know which must be secret and which must be shared before proceeding. • Use graphics throughout the asymmetric cryptography sections. It is much more complex than symmetric. • Setup the "rules of asymmetric": if something is encrypted with one key, it must be decrypted with the other.

4.3.3a EK: Public key encryption does not require the sender and receiver to share the same key.		• If the class is advanced, consider introducing Bitcoin with the video.
4.3.3c EK: Secret messages encipher the message with the recipient's public key, are sent, and then the recipient can decipher it using their private key.		• Walk through an example of using asymmetric cryptography to keep messages secret. • Ask students how this is different than symmetric cryptography, and what advantages asymmetric may provide.
4.3.3d EK: Digital Signatures are a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate.		• Walk through an example of using asymmetric cryptography to create digital signatures. • Ask students what are some uses of digital signatures. • Review these two methods before proceeding. Students should understand how asymmetric cryptography can be used two different ways to achieve different goals.
4.3.1k EK: Certificate authorities (CAs) issue digital certificates that validate the ownership.		• Demonstrate CAs in action by opening a web browser and navigating to a website. Click the details next to the URL to showcase the CA. Discuss web encryption and HTTPS.
8.1.1d EK: The loss of confidentiality is a critical factor in warfare.	• *Enigma M3*, https://www.101computing.net/enigma/ • Hinsley, Harry. "The Influence of ULTRA in the Second World War." 19 Oct 1993, http://www.cix.co.uk/~klockstone/hinsley.htm	• Practice hands-on decryption of realistic Enigma machine messages in the linked 101computing resource. • Emphasize cryptography's impact by explaining how breaking the Enigma codes shortened WW2 by 2-4 years.

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 forensics analyst.

UNIT 11: Authentication and Identity Management

Estimated Time in Hours: 7

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
4 Data Security 6 Adversarial Thinking 2 Establishing Trust	4.2	- Research the pros and cons of biometrics. - Examine where browsers store passwords. - Research password managers. - Explore user permissions on a Windows system.

Guiding Questions:

- What is identity and access management?
- Why should passwords be complex?
- What are the types of biometrics?
- What is multi factor authentication?
- What are single sign-on, federation, and transitive trust?
- Where are passwords stored?
- What are different types of access control?
- What is least privilege?
- What are groups, roles, privileges, & permissions?
- What are some dangers of social engineering?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
4.2.3d EK: Identity management includes authentication, access control, sometimes coordination across different domains, and management of the credentials throughout the lifecycle.	• Computer, lecture slides, projector, graphic organizers, access to Internet	• Provide the definition of identity management. Include identification, authentication, authorization, and accountability. A graphic organizer to help students differentiate among the terms is suggested, as these are terms students often confuse. • Take time to discuss each term and provide examples.
4.2.3a EK: Authentication is a process by which you verify that	• "Complex Passwords Harder to Crack, but It May Not Matter."	• Explain how passwords are a form of authentication. Discuss with students the characteristics of good passwords.

someone is who they claim they are. 4.2.3f EK: The strength of a password is a function of length, complexity, and unpredictability.	InetSolution blog, *inetsolution.com*, https://www.inetsolution.com/blog/june-2012/complex-passwords-harder-to-crack,-but-it-may-not • *How Secure Is My Password?* https://howsecureismypassword.net/	• Show students how easily passwords can be cracked. This can be by using a password cracker that you demo or using a chart like the one linked to the left. • Explain why password length matters (search space). • Discuss dictionary attacks. • Using How Secure Is My Password (linked on the left). Have students craft their own strong passwords.
6.1.4a EK: Human users of the system have their own conscious and unconscious objectives that can undermine cybersecurity protections and policies.	• "Password Minder Infomercial featured on Ellen." *YouTube*, uploaded by Consumer Affinity, Inc., 2 Jan 2019, https://www.youtube.com/watch?v=2HYmojdDweI&feature=emb_logo	• Show the video linked left about the Password Minder. Explain that this was a real product. Ask students their thoughts. Is it a good or bad idea? Why? • Have students list (or research) bad password habits that weaken security.
4.2.3c EK: Authentication can be done using multiple factors, something you have, something you know, something you do, & something you are. (E.g., have = card, know=password, do=sign, walk, are=fingerprint, retina)		• After discussing biometrics as a way to authenticate, have students research different types of biometric authentication. How does this strategy compare to passwords? • Discuss biometric related errors. • Discuss how users can authenticate using something they have.

		• Review authentication strategies something you know, are, or have. • Discuss multi factor authentication.
4.2.3 LO: Students will evaluate and recommend technical controls that can be used to secure data. 6.1.4 LO: Students will understand how social behaviors and human factors impact the cybersecurity of a system design	• Teravainen, Taina and Rouse, Margaret. "single sign-on (SSO)." TechTarget|SearchSecurity, *SearchSecurity.com*, https://searchsecurity.techtarget.com/definition/single-sign-on • Sheldon, Robert. "Explore the pros and cons of identity federation management." TechTarget|SearchMobileComputing, *SearchMobileComputing.com*, 23 Feb 2018 https://searchmobilecomputing.techtarget.com/tip/Explore-the-pros-and-cons-of-identity-federation-management • "QTNA #19: Transitive Trust." *YouTube*,	• Explain single sign-on to students. Ask students if they have ever used single sign-on. Have them list the advantages and disadvantages (see article linked left). • Contrast single sign-on with federation. Have students provide examples of federated accounts. Have students research the advantages and disadvantages to account federation (see source linked left). • Discuss transitive trust. The video linked left may help with this.

	uploaded by CyberVista, 20 June 2018, https://www.youtube.com/watch?v=uWifmuVOcLw&feature=emb_logo	
4.2.3b EK: Authentication requires a database of information.		• Ask students where passwords are stored. Explain that passwords have to be stored in a database somewhere. How can this be a vulnerability? • Have students investigate where browsers and Windows store passwords.
4.2.3g EK: Authorization is the process of establishing if the authenticated user, is permitted to have access to and/or act on a resource.		• Explain the concept of authorization. Compare it to their household. Does everyone in the house have the same authority (rights and privileges)? • Authorization is what you are allowed to do.
4.2.3i EK: Access Control is the process of enforcing the required security for a particular resource.		• Have students review the types of access controls from the previous units (MAC, DAC, RBAC, RuBAC). Review nondiscretionary and discretionary.
2.3.4a EK: A privilege is a right for the user to act on managed computer resources.	• "Unix / Linux – File Permission / Access Modes." tutorialspoint, *tutorialspoint.com*, https://www.tutorialspoint.com/unix/unix-file-permission.htm	• Review types of user privileges. The article linked left may help with this.
2.3.4 LO: Students will explore the principle of least privilege, which is about differentiating	• "What Is Privilege Escalation?" *YouTube*,	• Explain the concept of least privilege. Why is it important? Have students think of situations when least

among types of access control (mandatory, role-based, discretionary, and rule-based access controls) and analyzing which to use for selective restriction of access to a place or other resource. 2.3.4b EK: Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.	uploaded by Netwrix, 10 Jul 2018, https://www.youtube.com/watch?v=7PpYavvu-6k	privilege should be used. The video linked left is a resource for this concept.
4.2.3h EK: Groups, Roles, Privileges and Permissions are used to manage authorization.		• Explain groups, roles, privileges, and permissions. It is a good idea to map out how they relate.
4.2.3j EK: Failure to protect data can be due to faulty authentication, faculty authorization, and/or faulty access control.		• Discuss with students that these measures can fail. Have them use a Windows system to explore authorization.
2.3.4c EK: Granting only those privileges necessary for a user to accomplish assigned duties improves accountability and limits accidental misuse.		• Have students think back to their home. What happens if they do not do their chores? This is called accountability. Ask students how misuse can be spotted on a computer system. Discuss logging.

6.1.4b EK: Social engineering is one of the most widely used techniques in which an adversary compromises a system by convincing a human to violate the security policies in a way that enables the adversary to gain an advantage.	• "How to Spot a Phishing Email Attack – 5 key steps for 2020. SpamTitan from TitanHQ." *YouTube*, uploaded by TitanHQ Email Security and Web Security., 4 Dec 2019, https://www.youtube.com/watch?time_continue=34&v=P2TQmCcfD7Q&feature=emb_logo • @stewy6. "So I'm using Instagram's Question Stickers to ask ppl common password recovery questions, and most are actually responding #privacy @CryptoAustralia." *Twitter*, 23 July 2018, 2:03 a.m., https://twitter.com/stewy6/status/1017650779044265986	• No matter what controls are in place, a system is still vulnerable to social engineering. Discuss phishing and other techniques with students. Use the video linked on the left to guide discussion. • Show students the Tweet linked left. How does this link to passwords/password recovery?
8.1.1h EK: Cybersecurity events have led to the development of various cybersecurity career paths and various needs in order		• Discuss a potential related career path with students. Perhaps systems administrator.

to prepare people for these new types of jobs.		

UNIT 12: Why Is Software Vulnerable

Estimated Time in Hours: 6

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
1 Ethics 2 Establishing Trust 7 Risk 8 Implications	2.2	- Research the origin of specific vulnerabilities and how they detriment software. - Practice the basics of computer programming. - Investigate secure coding practices as a lead-in to the next unit.

Guiding Questions:

- Why are software development frameworks (DevOps, Agile) used?
- How does the principle of modularity relate to software development?
- How does the principle of simplicity relate to software development?
- Other than for security purposes, how does modularity and simplicity enhance software?
- How can an adversary alter a program's code?
- Why are software updates important?
- How can a developer's intentions differ from how their program is actually used by its consumer?
- Was the Internet designed with security in mind?
- What was the impact of the Morris Worm?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
7.2.3 LO: Students will be able to explain how the logical malleability of software and hardware can allow an adversary to change a system to meet the adversary's goals rather than the systems original objective.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Introduction to computer science as a career: "What Most Schools Don't Teach." *YouTube*, uploaded by Code.org, 26 Feb 2013,	• At the beginning of this unit, show the linked YouTube video which introduces computer science as a career. This is where students can begin simple computer programming (recommended IDE listed to the left). • Engage students in this unit by putting them in the shoes of a video game developer who rushes a game to launch and suffers from software vulnerabilities. Tie the solutions of these vulnerabilities to modularity and

	https://youtu.be/nKIu9yen5nc • Free, easy-to-use, web-based programming IDE: https://repl.it/ • DevOps: "The DevOps Revolution is Changing Cloud Security – Don't Get Left Behind." Check Point Software Technologies Ltd, *CheckPoint.com*, https://blog.checkpoint.com/2018/01/03/devops-revolution-changing-cloud-security-dont-get-left-behind/ • DevOps introduction video: "What is DevOps? – In Simple English." *YouTube*, uploaded by Rackspace Technology, 12 Dec 2013, https://youtu.be/_I94-tJlovg	simplicity to heighten the student's understanding of these principles. • Introduce DevOps (Development and Operations) or a similar development approach, such as Agile. Explain the main pieces of the lifecycle and anchor the rest of this unit to that development approach. • Ask students which stages of the DevOps/Agile framework and which piece(s) of the CIA Triad the vulnerabilities violate (e.g., if the game crashes frequently, this violates availability). • If given multiple software vulnerabilities, challenge the students to choose which problem is more important and should be addressed first.

2.3.7a EK: The principle of modularity says that individual components are capable of executing a unique part of the desired functionality and is achieved through system design. Because of this modular design, security upgrades can happen in one component without having to overhaul the entire system.		Note: modularity LO/EK is first referenced in Unit 7. • Review the principle of modularity. • Ask students to use modularity to repair one of the game's presented software vulnerabilities. • Other than fixing the software vulnerability, does adding modularity offer any other benefits?
2.3.7b EK: A system's components may be separated and recombined.		• Elaborate on enhancements modularity can provide the game, such as making it easier to add more game levels, new items, better communication features, etc. • If one of the modules breaks or experiences a vulnerability, do you necessarily need to repair the other modules?
2.2.1 LO: Students will describe the principle of simplicity, which is about ensuring that systems are easy to understand, maintain and test so as to be more secure. 2.2.1a EK: Simple designs are easier to understand, maintain and test for security problems.	• Vulnerability types: "Vulnerability Types – CompTIA Security+ SY0-501 – 1.6." *YouTube*, uploaded by Professor Messer, 14 Nov 2017, https://youtu.be/1UNCDsrDTu4	Note: simplicity LO/EK is first referenced in Unit 7. • Review the principle of simplicity. • Challenge students with using the principle of simplicity to repair one of the game's presented software vulnerabilities. • Task students to research the origin of specific vulnerabilities and why it can harm the software. You can task vulnerabilities from the linked YouTube video, or students can watch the video for ideas.

2.2 EU: The simpler you can make the design or implementation of a system, the better you can check whether or not it can be exploited. 2.2.1b EK: Simplicity is also known as "Economy of Mechanism."		• Other than the security benefits of simplicity, how does the principle of simplicity benefit the game in other ways? Students should relate the principle of simplicity to the scenario.
2.2.1c EK: A simple design incorporates a careful analysis of what is needed.	• UI comparison example: "New vs Old UI." Florida International University | Information Technology | PantherSoft, *FIU.edu*, 25 May 2018, https://panthersoft.fiu.edu/uiredesign/new-vs-old-ui/	• Explain the importance of simplicity in the design and functionality of user interfaces. • Ask students to judge which UI is best (example to the left) and determine which uses simplicity.
2.3.7 LO: Students will recognize that the cybersecurity often applies to a system that consists of individual self-sufficient components and the overall security is dependent on the security properties of the components.		• Relate this unit's scenario to the bigger picture. For example, the game consists of several smaller components: the user accounts, game servers, chat systems, etc. • Why do we need to protect each of these individually?
7.2.3a EK: Software is frequently updated to correct both	• "Why it's important to update your software | Update your phone [How	• Now that the student's game code has been repaired, the game itself must be tested, released and deployed (DevOps). Relate this to your chosen framework.

functional errors and security problems.	To] | Support on Three." *YouTube*, uploaded by Three UK, 29 Apr 2016, https://youtu.be/LkToKpX9ZWQ	• Explain the essential importance of software updates. • Show the linked YouTube video to your students. Ask them to list the reasons to update software.
1.2.2a EK: The designer assumptions and user assumptions could differ. Another way to say this, the user may not know the assumptions of the designer for using the tool, leading the user to use the tool in a way the designer never intended. 1.2.2 LO: Students will give examples of where/how tools are used in ways that were not intended by the system designer.	• List of ideas for activity: orange swan. "You've got an old computer, your're crafty, and you spent way too much time watching 'Transformers' as a kid." MetaFilter | Community Weblog, *MetaFilter.com*, 22 Oct 2012, https://www.metafilter.com/121155/Youve-got-an-old-computer-yourre-crafty-and-you-spent-way-too-much-time-watching-Transformers-as-a-kid	• Describe how software developers have to defensively code as users may use the software in ways the designer never considered. • Ask whether the students think it's a good or bad thing for people to find new ways to use software. Why or why not? • As an activity, show them photograph examples of things used in unintended ways. Ask them to identify the specific ways they are uniquely used.
7.2.3b EK: Software changes could come from an adversary that intentionally inserts code to meet the goals of the adversary. 7.2.3c EK: Changes in software code are common and those	• Insider Threat: "Insider Threats in 2 Minutes." *YouTube*, uploaded by Security Innovation, 11 Jul 2018, https://youtu.be/QXnNkSeT6dM	• Explain ways an attacker may attempt to change the source code itself through supply chain attacks or attacks against code repositories. • Show the linked YouTube video about insider threats and ask students these questions (a video viewing guide may be used).

introduced by an adversary are often not easily detected.		- How are insider threats dangerous? - Could an insider threat cause damage to source code? - How? - What are some ways to defend against insider threats?
8.1.1e EK: The violation of system integrity can alter the behavior of critical infrastructure.		• Changing software source code is an attack on its integrity. How would this impact critical infrastructure? • Assign students scenarios and have them research how a breach of integrity would harm the systems (e.g., source code damage to a COVID-19 case tracking app).
8.1.2b EK: Security was not seen as a concern until much of the "infrastructure" for computer networks was in place.	• Morris Worm: "Morris Worm explained." *YouTube*, uploaded by Cyber Security Entertainment, 7 Jul 2018, https://youtu.be/sm3wN8rLi8U	• Demonstrate the Internet's former lack of security by showcasing the Morris worm. Show students the linked YouTube video. • Use a video viewing guide to ask questions about the worm, such as how much monetary damage it caused, where it was launched from, and the type of modern cyber attack it inspired.
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 software developer.

UNIT 13: Software Vulnerabilities

Estimated Time in Hours: 10

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
1 Ethics 2 Establishing Trust 5 System Security	5.3	- Research, summarize, and list examples of specific vulnerability types. - Research insecure cryptographic algorithms and provide secure replacements for them. - Create summary videos of how security best practices mitigate or prevent software vulnerabilities. - Advanced students will code and demonstrate buffer overflow vulnerabilities in the C programming language.

Guiding Questions:

- Why are CVE and OWASP beneficial to the security community?
- What is an injection attack? What does it do?
- How can buffer overflow attacks be prevented?
- Is cryptography, regardless of what kind, a guaranteed way to secure data?
- What is the SSDLC and how does it differ from old software development methods?
- What is the difference between static and dynamic analysis?
- What are zero-day attacks and why are they so devastating?
- Are zero-day attacks always discovered by adversaries?
- Why is patching so important?
- How is process isolation essential to security?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
5.3 EU: Security vulnerabilities in software are weaknesses in a system's design, implementation, or operation and management	• Computer, lecture slides, projector, graphic organizers, access to Internet	• Review software vulnerabilities. • Ask students why software is vulnerable (review of Unit 12).

that could be exploited to violate the system's security policy.		
5.3.1 LO: Students will describe common security-related software vulnerabilities. 5.3.3b EK: Security vulnerability reports such as Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE) are publicly available for software systems and should be monitored, or subscribe to their alerts.	• CVE Explanation in 90 seconds: "What is Common Vulnerabilities & Exposures (CVE)." *YouTube*, uploaded by F5 Inc., 2 Feb 2020, https://youtu.be/qfpnJyTl1To • CVE Charts: "Vulnerabilities By Type." CVE Details, *CVEDetails.com*, https://www.cvedetails.com/vulnerabilities-by-types.php • OWASP Top 10: "OWASP Top Ten Web Application Security Risks." Open Web Application Security Project, *OWASP.org*, https://owasp.org/www-project-top-ten/	• Introduce the Common Vulnerabilities and Exposures (CVE) as a way to categorize, track, and share information about vulnerabilities. • Show the linked YouTube video explaining CVEs. Use a video viewing guide. • Show the CVE statistics. Ask students why they think certain vulnerability types are more prevalent and how those change over the years. • Explain the OWASP (Open Web Application Security Project) Top 10 security risks against web applications. • Challenge students with an independent activity to research, summarize, and list examples of specific vulnerability types.

5.3.1a EK: Injection attacks occur when an external source such as a user provides input that causes a program to behave in ways that violate the security policy by executing harmful commands. 5.3.1c EK: A software vulnerability may exist when data is allowed to include unauthorized control instructions that dictate how the program should behave and thus can cause the program to behave in a way that violates the security policy.	• OWASP #1 Vulnerability (Injection Attacks): "OWASP Top 10: Injection Attacks." *YouTube*, uploaded by F5 DevCentral, 13 Dec 2017, https://youtu.be/rWHvp7rUka8	• Introduce injection attacks. As many injection attacks focus on SQL injection, you should consider covering SQL database basics as well. • Show the linked YouTube video explaining the OWASP #1 (Injection Attack). Use a video viewing guide to assess their learning. • Ask students how they think injection attacks can be prevented. They will learn more on this later.
5.3.1b EK: A buffer overflow is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations, and how this can be used as an entry point by an attacker to violate security policy.	• Interactives for Buffer Overflow / SQL Injection: "Cybersecurity Interactives." E-Mate 2.0, *e-mate-bbc.org*, https://s3.amazonaws.com/e-mate2/Cybersecurity+Interactives/Cybersecurity+Interactives.html • Buffer Overflow overview: "Ethical Hacking: Buffer Overflow Basics."	• Show the linked YouTube video explaining Buffer Overflow attacks. Use a video viewing guide to assess student learning. • Ask students how they think buffer overflows can be prevented or at least reduced. The video covers some tactics.

	YouTube, uploaded by National Consortium for Mission Critical Operations, 24 Nov 2014, https://youtu.be/SOoJcrR4Ijo	
5.3.1d EK: A software vulnerability may exist when cryptographic functions are not implemented properly or when the cryptographic functions are assumed to provide more security than the algorithm provides.		• Review how cryptography can protect systems. Although this may seem like a security catch-all, that can be deceiving. • Emphasize that just because cryptography exists, doesn't mean the data is secure. Cover insecure or improperly setup cryptography. • Task students with researching cryptographic algorithms no longer considered secure. They can summarize why it is no longer considered secure and list any secure replacements.
5.3.1e EK: Changes to the environment can cause software to no longer meet the security policy and secure software must include considerations for how to implement future changes (e.g., credentials, algorithms, and patching code to correct bugs and errors).		• Explain how secure environments require any new software or updates to be verified and tested for both security and functionality. • Ask students whether they think this is good or bad. The process may slow down new additions to the environment, but ultimately it acts to its benefit.
5.3.1f EK: A software vulnerability can occur when external components that don't		• A secure environment will often limit what can be connected to them. For example, they may not be able to

meet the security policy requirements are connected to the system.		connect with USB drives, CDs, or other computer networks. • Ask students why these restrictions are in place. Does it make the environment more secure? How do they enforce it?
5.3.2 LO: Students will identify the processes of developing secure software.	• Secure Software Development Life Cycle: "Secure Software Development Lifecycle." Digital Maelstrom, *DigitalMaelstrom.net*, https://www.digitalmaelstrom.net/security/secure-software-development-lifecycle-ssdlc/	• Introduce a framework for developing secure software, such as the Secure Software Development Life Cycle (SSDLC). • The SSDLC differs from many other frameworks in that it requires security throughout the entire process. Each stage of the original SDLC (without security) now requires essential security actions. • Ask students why it is important to consider security throughout the entire development and operation of software. Relate this to the scenarios in Unit 12.
5.3.2a EK: Input validation is code added to the program that verifies input provided by an external source is the type of input expected and will be processed correctly.	• Student-made video explaining input validation: "Input Validation." *YouTube*, uploaded by CLARK Cybersecurity Curriculum Digital Library, 10 Sep 2015, https://youtu.be/-8bDdrZhj_k	• Review how software developers have to anticipate how end users will abuse their software and use it in other ways. • Task students with creating their own summary videos of how security best practices (i.e., input validation) mitigate or prevent software vulnerabilities. A linked YouTube video is provided to the left as an example.

5.3.2b: EK Static analysis of software is a process in which external tools analyze the code and automatically identify potential security vulnerabilities such as potential buffer overflows.	• Static Analysis explanation: "What Are Static Analysis Tools?" *YouTube*, uploaded by goobar, 19 Oct 2018, https://youtu.be/d_BCGvXbpKs	• Explain static analysis as an important piece of SSDLC. Code should be routinely examined as it is developed. • For more explanation, show the linked YouTube video to overview static analysis. Use a video viewing guide to review. • Showcase some insecure coding practices or functions (e.g., buffer overflows in the C programming language) as examples which static analysis can detect.
5.3.2c EK: Development tools and Integrated software Development Environments (IDE)s provide static analysis tools to check for some types of insecure code such as identifying potential buffer overflows.		• Provide examples of static analysis tools. Ask students to compare and contrast.
5.3.3 LO: Students will describe the process of validating that software remains secure through its lifecycle. 5.3.3a EK: A security analysis is a process that is used to verify a program meets a specified list of security requirements.		• Describe how software needs to be validated and secured even after its development. Ask students why this is important. • The SSDLC is one framework that provides security analysis. Use this or a similar framework as an example.
5.3.3c EK: A zero-day vulnerability is a software security flaw that is unknown to people who should be	• Zero-Day Attack: "Anatomy of an Attack – Zero Day Exploit." *YouTube*, uploaded by	• Even if software is secure at launch, it can become subject to a zero-day vulnerability at any point. This is one reason why constant security is necessary even after software is developed.

responsible for patching or fixing the flaw.	FireEye, Inc., 19 May 2015, https://youtu.be/-BIANfzF43k	• Show the linked YouTube video about zero-day exploits. Why are zero-day attacks so devastating? Are zero-day exploits always found by an adversary?
1.3.3d EK: Disclosure of software vulnerabilities to a party other than the software developer is legal and can be harmful.		• Explain how security researchers search for zero-day vulnerabilities before adversaries. They seek to find and report these bugs before they are reported. • Discuss bug bounties and how companies will often pay for the discovery and discrete disclosure of bugs.
5.3.3d EK: Managing vulnerability reports, patching and patch distribution is a key part of software security.		• Review the importance of updates from Unit 12. Patching is synonymous with updates. Ask students why patching is essential, especially in the wake of zero-day attacks?
5.3.3e EK: Dynamic analysis is a process in which external tools analyze the execution of code in order to automatically identify potential security vulnerabilities.		• Contrast dynamic analysis with static analysis. • Ask students why it is important to test the software in both its execution and raw code states.
2.3.2 LO: Students will know that the principle of process isolation prevents tampering or interference from/by other processes. 2.3.2a EK: A process is a program running on a computer.		• Review processes and the principle of process isolation. • Why is process isolation important to the security of programs?

2.3.2b EK: Each process has a region of the memory (address space), which only it can access. 2.3.2c EK: Processes have to use defined communications mediated by the operating system to communicate with other processes.	• Buffer Overflow programming practice: "CSC 5991 Cyber Security Practice | Lab 2: Buffer Overflows." Wayne State University College of Engineering, *Wayne.edu*, http://webpages.eng.wayne.edu/~fy8421/16sp-csc5991/labs/lab2-instruction.pdf	• Explain how the operating system will distribute memory to the processes. How can this be exploited in attacks like the buffer overflow? • Advanced programming students may practice a buffer overflow example in the C programming language (linked to the left).
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 secure software assessor.

UNIT 14: OSI Model

Estimated Time in Hours: 8

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 3 Ubiquitous Computing	3.1	- Compare and contrast TCP and UDP and research their use cases. - Use Wireshark to examine the layers of the OSI model in network packets.

Guiding Questions:

- Why is the OSI Model broken into separate layers?
- What are some connection mediums used at the physical layer?
- What is the difference between TCP and UDP?
- When are TCP connections used?
- When are UDP connections used?
- How is the OSI model an abstraction and how is that useful?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
3.1 EU: The Internet is a large, globally distributed network that is divided into layers, governed by protocols, and connects a wide variety of devices.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Scope of the Internet: "Part 1: How big is the Internet?" *YouTube*, uploaded by Sebastian König, 4 July 2014, https://youtu.be/zl6B3KWRq8s	• Show the linked YouTube video to demonstrate the scope of the Internet. • Ask students how these computers are connected. How are all the communications managed?

3.1.1 LO: Students will explain how devices use layers to communicate across the Internet and describe the purpose of the layers.	Interactive breakdown of the OSI model: "Cybersecurity Interactives." E-Mate 2.0, *e-mate-bbc.org*, https://s3.amazonaws.com/e-mate2/Cybersecurity+Interactives/Cybersecurity+Interactives.html • OSI Model explained: "OSI Model Explained | Real World Example." *YouTube*, uploaded by CertBros, 28 Sep 2016, https://youtu.be/LANW3m7UgWs	• Describe how we use models to describe and standardize how information travels from one computer to another. Compare the OSI model to the TCP/IP model. This unit will focus on the OSI model. • Review mnemonics for memorizing the stages: "Please, Don't Need Those Stupid Packets Anyway." Ask students to create their own mnemonic. • Show the interactive breakdown of the stages of the OSI model (linked to the left). • The OSI Model video can either be shown as a preview, post-lesson review, or in pieces at the specific layers.
3.1.1a: EK Networks carry two types of information, those that allow for the controlling of the data and the data itself.		• Explain how some network traffic controls how traffic is transported across on a network. Packets use headers to classify the kind of information it carries and to pass information across all layers. • Students may understand an analogy to the mail system. When a letter it mailed, the message you want to send is inside the envelope. The information outside the envelope (address & stamp) controls how the data is sent.

3.1.1b EK: Physical links include optical cables that send signals using light, cables that send signals using electrical pulses, and wireless networks that send signals over radio waves.		• Describe how the physical layer is what carries everything from point-to-point. • Show students cables, network cards, Wi-Fi access points, etc. Making this into a show-and-tell of the physical layer will make the experience more memorable. • Ask students to explain why this layer is an important one to begin with.
3.1.1c EK: Link layer protocols such as Ethernet, Wi-Fi (e.g., 802.11), and Bluetooth are specific to the physical layer connection and describe how the signals are used to exchange data between the devices.		• Explain how the link layer protocols support the physical layer. • Ask students why it is important for the OSI model to include protocols that support the physical layer. Does the physical layer have any digital aspects?
3.1.1d EK: The network layer connects different types of physical/link layer networks into a single global Internet that transmits data from one computer to another using packets and logical addressing.		• Be sure to note that the network layer is where computers talk to each other. This handles the routing and connection between systems. • Without the network layer, the Internet would not exist.
3.1.1e EK: Once a packet arrives at a device, the transport layer uses port numbers to determine which application (web browser, email app, game, etc.) receives the packet, allowing for the reliable delivery of data between	• TCP vs UDP comparison: "TCP vs UDP Comparison." *YouTube*, uploaded by PowerCert Animated Videos, 15 Nov 2016,	• The transport layer helps ensure your data is transported from computer A to computer B in one piece. • Explain the TCP and UDP protocols here. Show the linked YouTube video with a video viewing guide.

a sending and receiving application.	https://youtu.be/uwoD5YsGACg	• Task students with researching the difference between TCP and UDP. • When should TCP be used? What is its advantage? • When should UDP be used? What is its advantage? • Port numbers should also be taught here and framed as the method used to make sure specific applications get the data they need.
3.1.1f EK: Internet and device applications (web, text messaging, games, etc.) follow protocols at the application layer (e.g. http, sms, proprietary protocols, etc.).	• OSI Layers in action: "Introduction to the OSI Model." *NetworkLessons.com*, https://networklessons.com/tag/osi/introduction-to-the-osi-model	• If teaching the OSI model, this should cover layers 5-7 (session, presentation, and application). In TCP/IP, this is solely the application layer. • This layer handles things like e-mail, web browsing, file transfers, etc. • Have students use a tool like Wireshark to view the different layers in action. The link to the left has a guide for this.
2.2.2 LO: Students will use the principle of abstraction to represent complicated concepts more simply and to allow solutions to be transferred to other contexts. 2.2.2b EK: Good and elegant design involves using abstraction.		• Explain how the OSI model uses abstraction to categorize the layers. In real application, the layers are a bit muddled and tend to represent the TCP/IP model. • How can the OSI model as an abstraction assist with troubleshooting network and communication problems?

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 IT auditor.

UNIT 15: Network Standards & Protocols

Estimated Time in Hours: 8

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 3 Ubiquitous Connectivity		- Use nslookup to test their understanding of DNS. - Research, identify, and categorize open-source and proprietary protocols.

Guiding Questions:

- How are protocols different from standards?
- What is the purpose of DNS?
- What is the value of open-source protocols?
- Are proprietary protocols necessarily more secure?
- What is security by obscurity? Is it effective?
- How do protocols implement minimization?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
3.1.2 LO: Students will explain how network standards and protocols allow different types of devices to communicate.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Reference comparison between protocol and standard: • Rusev, Emanuil. “What’s the difference between the terms ‘protocol’ and ‘standard’?” Stack Exchange | Software Engineering,	• Differentiate standards vs protocols here. Protocols are like languages, while standards are like dictionaries.

	StackExchange.com, 2 Sept 2011, https://softwareengineering.stackexchange.com/questions/105449/whats-the-difference-between-the-terms-protocol-and-standard	
3.1.2a EK: Communication protocols define the rules, types, and formats of messages exchanged between devices and are necessary to allow devices to communicate with each other.	• Simple protocol explanation: "Computer Networking Tutorial – 10 – What is a Protocol?" *YouTube*, uploaded by thenewboston, 11 Dec 2012, https://youtu.be/VlKksZhI0	• Ask students to list protocols they know about: TCP, UDP, HTTP, HTTPS etc. • The YouTube video linked to the left is a simple explanation of how a protocol works.
3.1.2b EK: Protocols like the Domain Name System (DNS) provide a mechanism to map names like "www.example.com" into numbers (IP addresses), similar to a phonebook that maps names to phone numbers.	• DNS overview: "How a DNS Server (Domain Name System) works." *YouTube*, uploaded by PowerCert Animated Videos, 26 May 2016, https://youtu.be/mpQZVYPuDGU • Activity: use the command window tool	• Explain how DNS is a useful protocol used for navigating to websites without knowing its IP address. • Show the YouTube video linked to the left and use a video viewing guide to assess learning. • Challenge students by having them use *nslookup* to identify domain names or their corresponding IP addresses.

	nslookup to check the DNS-mapped IP addresses of domain names. Examples: "Using Nslookup." Get Certified Get Ahead, *gcgapremium.com*, https://gcgapremium.com/using-nslookup/	
3.1.2c EK: Some protocols are proprietary and are available only to authorized users while other protocols are published as formal standards and allow devices from any manufacturer to communicate with each other. 3.1.2d EK: Some standards are open standards where the packet format and message exchange rules are available to everyone. In other standards called proprietary standards, the message formats and message exchange rules are only provided to authorized entities.		• Contrast open-source vs proprietary software. • Open-source software gets a larger pool of supporters who can review and suggest changes to the source code. Ask students if this is a good thing or bad thing. Does it enhance security? • Explain how open-source protocols are often more popular because they can be implemented freely and often more easily than proprietary counterparts. • As a research project, have students identify protocols that are open-source and proprietary.
3.1.2e EK: When designers rely on secrecy, assuming an adversary cannot compromise the system because the adversary cannot determine how	• Security by obscurity analogy: "Security via Obscurity Is a Bad Idea." *YouTube*,	• Explain the misconception of "security by obscurity." For example, you may be tempted to hide an insecure service by changing its port number; however, adversaries can

the system works is known as security through obscurity. It is widely accepted that security through obscurity should never be your only security mechanism.	uploaded by Phil Koopman, 10 Nov 2018, https://youtu.be/FR9YZlmeojY	still detect the actual service running on the misleading port number. • Ask students if leaving a key under your doormat is secure. Adversaries know how to check there, but in cyberspace they also have the capability to write a script to check under door mats for them. See the video for a full explanation of this analogy.
3.1.2f EK: Cryptographic algorithms are either publicly known or proprietary. The use of proprietary cryptographic algorithms is largely discredited, as evidenced by organizations like NIST, which encourages public review of algorithms.		• Ask students if cryptographic algorithms should be public or private knowledge. • Explain the security of cryptography lies in the power of the algorithm, not its secrecy. The process of encryption is not secret, only the key and plaintext should be secret.
3.1.2g EK: Through experiments, an adversary can often learn how proprietary protocols or algorithms work even though the adversary is not an authorized user.		• Why does it not help to keep the protocol/algorithm secret? • Adversaries can use the tactic of reverse engineering to discover how the algorithms function. Keeping it secret does not protect it. • Note that when software is open-source or public, the community's feedback can help make it more secure or reveal its flaws for patching.
2.2.3 LO: Students will apply the principle of minimization by decreasing the number of ways		• Ask students why there are so many protocols.

in which attackers can exploit a program or device. 2.2.3a EK: The attack surface of a software environment is the sum of the different points where an unauthorized user can try to enter data or to extract data from an environment. 2.2.3b EK: Minimizing the attack surface decreases the opportunity to find an exploitable vulnerability in the system. 2.2.3c EK: The human interface should be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. 2.2.3d EK: Common mechanisms and access should be minimized.		• Protocols should be fairly narrow-focused to follow the principles of minimization. By following rules and a narrow use-case, minimization allows protocols to lower possible attack vectors. • Review the principle of minimization. • What is the purpose of HTTP? To provide web pages. • What is the purpose of FTP? To transfer files. • What is the purpose of RDP? Command and control a computer remotely. • Explain how in the case of complicated protocols, they often borrow features from other protocols. For example, HTTPS uses the SSL/TLS protocol to provide security for web browsing.
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 incident responder.

UNIT 16: Complexity of Cyberspace

Estimated Time in Hours: 7

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
6 Adversarial Thinking 7 Risk	7.2, 6.1	- Research and map the components of a complex system. - Research major Internet milestones. - Experiment with HTML and learn about HTTPS.

Guiding Questions:

- What is a complex system?
- What is the output of a complex system?
- What causes a system to change?
- How is cyberspace complex?
- What is the Internet?
- Who owns the Internet?
- Who hands out IP addresses?
- How/Why does the Internet change?
- What are attacks against the Internet?
- Do people always use things the way they are intended?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
6.1.1b EK: Complex systems typically have input from many sources and are highly changeable. 7.2.1a EK: A complex system is a system composed of many parts, which may interact with each other, where the interactions	• Computer, lecture slides, projector, graphic organizers, access to Internet	• Explain to students the meaning of a complex system and how that systems do can be complex without being complicated. • Have students list all the technology used as school (including apps). Next, have them map the ways the technology is connected.

produce properties that its parts do not have.		• Ask them if any of the technology ever changes (updates, new equipment, new rules, is phased in or out, etc.). How do these changes happen? • Ask students what the product is of the system. Possible answers: graduates, learning, educated people. Ask if any one of those components, without the help of the rest, could produce this product. • Ask students to map their own version of a complex system. This could be a hospital, bank, grocery story, etc.
7.2.1c EK: The behavior or output of cybersystems cannot be predicted simply by analyzing the parts and inputs of the system. 7.2.1d EK: The behavior of the system is emergent and changes with time. The same input and environmental conditions do not always guarantee the same output. 7.2.1b EK: The behavior of complex systems has unpredictable output, i.e., it is intrinsically difficult to model due to the dependencies, competitions, relationships, or other types of interactions		• Note that it is the parts working together that determines the behavior or output. Just the individual elements cannot produce it by itself. • Discuss the essential knowledge statements. • Have students note that the behavior of system changes with time and has different outputs. For example, they may receive a different education than their brothers, sisters, or parents. Also, students who sat in the same classroom will use the knowledge attained different ways. There is no way to predict which students will become doctors or which ones will become teachers. • Have them apply this with their version of a complex system.

between the parts or between a given system and its environment.		
7.2.1e EK: The participants or agents of a system (human agents, including or especially adversaries, in this case) are self-learning and change their behavior based on the outcomes of the previous experience.		• Ask students why systems change. Note that teachers often adjust the way they teach to meet the needs of the learner. Grocery stores may change their layout to improve sales. Adversaries change their techniques to match the weaknesses of a system.
7.2.1 LO: Students will be able to explain how cyberspace is a very large, complex system of cybersystems that include hardware, software, social, economic, and political components. 6.1.1 LO: Students will explain how cybersystems are complex systems. 6.1.1a EK: A complex system is a system composed of many components which may interact with each other.	• "TRADOC Pamphlet 525-7-8: The United State Army's Cyberspace Operations Concept Capability Plan 2016-2028." Federation of American Scientists, *FAS.org*, https://fas.org/irp/doddir/army/pam525-7-8.pdf	• Note that the Internet is a complex system. List the components for students (hardware, software, social, economic, and political). Have them think of examples. • Building on these components, discuss what makes it a complex system. • Have students explore how the components interact. Using the document linked left, explore the layers on page 8 and the infrastructure relationships on page 12.
6.1.1c EK: The internet is a prime example of a complex system in that it is a large and complex	• "What is the Internet? (video)" Khan Academy, *KhanAcademy*.org,	• Use the video linked on the left to discuss the complexity of the Internet.

system composed of multiple, dispersed, independent systems.	https://www.khanacademy.org/computing/computer-science/computers-and-internet-code-org/internet-works-intro/v/what-is-the-internet • "TRADOC Pamphlet 525-7-8: The United State Army's Cyberspace Operations Concept Capability Plan 2016-2028." Federation of American Scientists, *FAS.org*, https://fas.org/irp/doddir/army/pam525-7-8.pdf • "Khan Academy and Code.org | Wires, cables, and WiFi." *YouTube*, uploaded by Khan Academy Partners, 30 July 2018, https://www.youtube.com/watch?v=qtmTMvXKKdg&feature=emb_logo	• Discuss who owns the internet. See page 11 of pdf linked left. • Discuss wires, cables, and Wi-Fi. Use the video linked left to guide the discussion. • Use the Bits and Bytes activity on the left to discussion how information transmitted across the Internet. • Discuss cellular networks. • Explain IP Addresses and DNS. Use the video on the left for this discussion. Use the activity linked left to help with student understanding. • Discuss packets, routers, and reliability. Use the video linked left to guide this discussion. • Discuss with students who hands out IP addresses. • Using Speedtest.net (linked left), have students run a speed test on their computer. Explain the results. • Discuss HTTP and HTML. Use the video linked left to assist with this. • Allow students to experiment with HTML using w3schools.com (linked left). • Have them do the HTTP activity linked left.

	• McNamara, Sherri. "Computer Technology AMI4: Bits and Bytes Activity." Greene County Tech School District, *gctsd.k12.ar.us*, https://www.gctsd.k12.ar.us/images/AMIPackets/JHS/McNamara/PCTech/AMI4.pdf • "IP addresses and DNS | Internet 101 | Computer Science | Khan Academy." *YouTube*, uploaded by Khan Academy, 23 Apr 2019, https://www.youtube.com/watch?v=MwxMsaFFycg&feature=emb_logo • "CS Principles 2019-2020 | Unit 1 | Ch. 2 | Lesson 12: The Need for DNS." *Code.org*, https://curriculum.code.org/csp-19/unit1/12/ • "Packet, routers, and reliability | Internet 101 | Computer Science | Khan Academy."	

	YouTube, uploaded by Khan Academy, 23 Apr 2019, https://www.youtube.com/watch?v=aD_yi5VjF78&feature=emb_logo • "Speedtest Global Index." *Speedtest.net*, https://www.speedtest.net/global-index#mobile • • "HTTP and HTML | Internet 101 | Computer Science | Khan Academy." *YouTube*, uploaded by Khan Academy, 23 Apr 2019, https://www.youtube.com/watch?v=1K64fWX5z4U&feature=emb_logo • "Tryit Editor v3.6." *W3Schools.com*, https://www.w3schools.com/html/tryit.asp?filename=tryhtml_intro • "CS Principles 2018 | Unit 1 | Ch. 2 | Lesson 13: HTTP and Abstraction	

	on the Internet | Worksheet - HTTP in Action." *Code.org*, https://docs.google.com/document/d/1zAaHDXi00V4ewphP8w2A41hF-9Fj3Sjg8c6oPbez254/edit	
6.1.1c EK: The internet is a prime example of a complex system in that it is a large and complex system composed of multiple, dispersed, independent systems.	• Routley, Nick. "The 20 Internet Giants That Rule the Web." Visual Capitalist, *VisualCapitalist.com*, 5 Jan 2019, https://www.visualcapitalist.com/20-internet-giants-rule-web/	• Have students list ways the Internet has changed. The graphic linked left is a good illustration of this.
7.2 EU: There are factors that necessitate cybersecurity risk as emergent and complex: the presence of an adversary, the logical malleability of computers, and the decentralized and distributed nature of networked systems. 1.2.2a: The designer assumptions and user assumptions could differ. Another way to say this,		• Discuss EU 7.2 (at left). Have students think of examples to support this. • Have students brainstorm ways adversaries can use cyberspace (recruitment, propaganda, training, command and control). How does this depart from the original intent of the Internet? Discuss the ethical implications of this. • Using the Dyn attack of 2016, discuss the importance of DNS. Who was impacted as a result of the attack?

the user may not know the assumptions of the designer for using the tool, leading the user to use the tool in a way the designer never intended. 6.1 EU: Adversity comes from anyone or anything where the end result differs from that intended by the system designer and user.		
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.		• Tie this unit to a career, such as a system requirements planner.

UNIT 17: Why Is the Internet Vulnerable

Estimated Time in Hours: 7

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
3 Ubiquitous Connectivity 1 Ethics	3.2, 3.1	- Research a SOC. Use a vulnerability scanner. - Research the dimensions of Cyber Warfare (Army Cyber Operations).

Guiding Questions:

- What would life be like without the Internet?
- What would it take for the entire Internet to fail?
- How are we targets?
- What can an attacker see?
- How long can an attack last?
- What can an attacker do?
- Who protects the Internet?
- What are the dimensions of cyber warfare?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
3.2 EU: The Internet provides a large attack surface, which offers efficiencies or economies of scale for adversaries.	• Computer, lecture slides, projector, graphic organizers, access to Internet • "What Would Happen If America's Internet Went Down." *YouTube*, uploaded by Tech Insider, 12 June 2018, https://youtu.be/eHfU3W-ClTE • Nakashima, Ellen. "Russian military was	• Have students imagine what would happen if the entire Internet went down. Discuss this. • Show the video linked left. Have students note the 5 core processes. Why would an attacker choose to attack these? • The video mentions Notpetya. Have students read the article linked left. What was the target of the attack? Who was behind it? Why? What was the purpose of the attack? What is a watering hole attack?

	behind 'NotPetya' cyberattack in Ukraine, CIA concludes." The Washington Post, *WashingtonPost.com*, 12 Jan 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html	• Discuss things that could take out the Internet (asteroid collision, global war, solar flare, massive cyber attack). Which are more likely? Why?
3.2.1 LO: Students will analyze how the connected nature of the Internet allows an adversary to reach a large number of devices. 3.2.1b EK: By directing an attack at a collection of devices (or even all devices on a network), an adversary can attack multiple devices simultaneously, in hopes of compromising a few select devices.	• "Cybersecurity and crime | Internet 101 | Computer Science | Khan Academy." *YouTube*, uploaded by Khan Academy, 23 Apr 2019, https://www.youtube.com/watch?v=5k24We8pED8&feature=emb_logo • Crane, Casey. "DDoS Attacks | Re-Hash: The	• Have students investigate the connected nature of the Internet. • Discuss how this connectiveness allows an adversary to reach a large number of devices. • Show video linked left. Discuss ways we are all targets. • Discuss how an adversary can attack multiple devices simultaneously.

3.2.1c EK: An adversary can attack a large number of systems simultaneously, which can impact a large majority of a group of people.	Largest DDoS Attacks in History." Hashed Out, *TheSSLStore.com*, 25 June 2020, https://www.thesslstore.com/blog/largest-ddos-attack-in-history/.	• Discuss how an adversary can attack large systems simultaneously. What are the results of these types of attacks? • Have students read the article on DDoS attacks (linked left). Students should note the how DDoS attacks are measured (packets and bandwidth), types of DDoS attack methods, and pick a DDoS attack listed and summarize it.
3.2.1a EK: Network mapping and recon tools allow an adversary to gain information on remote systems and an opportunity to get control of the system.	• "Greenbone Security Manager Live Demo." *Greenbone.net*, https://livedemo.greenbone.net/login **Username: livedemo / Password: livedemo**	• Ask students what they think an attacker can see during an attack. • Discuss network mapping, network reconnaissance, and vulnerability scanning. Offer example tools of each and explain their purpose. How could these tools aid an attacker? How does a network administrator use this information? Greenbone security, linked left, offers a free live demo of their vulnerability scanner. Allow students to experiment with it or the teacher can use it as a demo and explain how it works.
3.2.1d EK: An adversary can stay undetected for a long period of time suggesting that early detection is key in preventing a large amount of damage. 3.2.2 LO: Students will identify and predict the outcomes of security vulnerabilities at the physical/link layer, the network	• "2019 Cost of a Data Breach Report | Data Breach Calculator." IBM, https://databreachcalculator.mybluemix.net/?_ga=2.268380235.494425760.1589305840-1006873831.1589305840&cm_mc_uid=94402621085815893058404	• Ask students how long they think an attack can last. Have students research the breach report linked left. • Ask students what an attacker can do once he/she gains entry into a system. Discuss vulnerabilities at each level of the OSI model mentioned in the EKs. The resource linked left offers excellent resources for exploring attacks related to these vulnerabilities.

layer, the transport layer, and the application layer. 3.2.2a EK: At the physical/link layer, an adversary who is able to connect to the link can observe, and possibly modify or jam messages on that link. 3.2.2b EK: At the network layer, an adversary may do two things, impersonate an address (spoofing) or disrupt communication (Denial of Service). 3.2.2c EK: At the transport layer, an adversary may disguise their intentions by using port numbers incorrectly or may disrupt the ability of a device to deliver data to the application. 3.2.2d EK: At the application layer, messages sent by the adversary may cause applications to stop working or behave in a way that serves the goals of the adversary, rather than the way they were designed.	&cm_mc_sid_50200000=95192341589305840431&cm_mc_sid_52640000=53766491589305840462 • "Cybersecurity Interactives." E-Mate 2.0, *e-mate-bbc.org*, https://s3.amazonaws.com/e-mate2/Cybersecurity+Interactives/Cybersecurity+Interactives.html	

1.1.2 LO: Students will understand how the role of values and ethics affects political structures, laws, and policy decisions as it relates to cybersecurity. 1.1.2e EK: Professional codes of ethics convey the expected conduct of cybersecurity professionals. 1.1.2b EK: Institution refers to informal norms, shared understandings, and formal doctrines that constrain and prescribe actors' interactions with one another. 1.1.2c EK: Cyberwarfare, cybersecurity and privacy affect and are affected by institutions, political structures and attendant policies. 1.1.2a EK: Political structure refers to institutions, their relations to and interactions with each other, and the laws and norms present in political systems in such a way that they	• "Code of Ethics." EC-Council, *ECCouncil.org*, https://www.eccouncil.org/code-of-ethics/ • "Team Red vs. Team Blue and how to get into Cyber Security – with Brad Wolfenden." *YouTube*, uploaded by Coding Blonde, 10 Nov 2018, https://youtu.be/Mmd_56Y-1Cc • Firch, Jason. Red Team VS Blue Team: What's The Difference?" PurpleSec, *PurpleSec.us*, https://purplesec.us/red-team-vs-blue-team-cyber-security/ • Borkar, Pramod. "Security Operation Center: Ultimate SOC Quick Start Guide." Exabeam, *Exambeam.com*, 24 Jan 2019, https://www.exabeam.com/security-operations-	• Ask students who protects the Internet. How? Discuss that decisions regarding cyber attacks are complex and involve ethics, political structures, laws, and policy. • Focus on the role of ethics in these decisions. Have students read the code of ethics linked left. • Discuss the role of political structures, laws, and policies. • Discuss the role of a red team versus a blue team. Why are both important? Show the video linked left to help students answer this question. Have students read the article linked left. • Using the article linked left, research a Security Operations Center (SOC). Have students map out their own.

constitute the political landscape of the political entity. 1.1.2d EK: Cybersecurity laws reflect values about national security, economic security, welfare of citizens, domestic law and order, and legitimacy of government.	center/security-operations-center-a-quick-start-guide/	
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.	• "The Army Cyber Team." *YouTube*, uploaded by U.S. Army Cyber Command, 18 Oct 2017, https://www.youtube.com/watch?v=IkAwYGXqBz4 • "TRADOC Pamphlet 525-7-8: The United State Army's Cyberspace Operations Concept Capability Plan 2016-2028." Federation of American Scientists, *FAS.org*, https://fas.org/irp/doddir/army/pam525-7-8.pdf	• Remind students that cyber attacks can sometimes result in cyber warfare. Show video linked left. • Using the document linked left, have students research Arm Cyber Operations and the three dimensions of cyber warfare. They should define CyberSA, CyNetOps, CyberWar, and CyberSpt, explaining the role of each and how they interact. • Students should examine a NICE work role. Perhaps communications security manager.

UNIT 18: Cyber Attack Kill Chain

Estimated Time in Hours: 6

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
7 Risk 6 Adversarial Thinking 8 Implications	7.2	- Identify potential adversaries & their motivations. - List & define common system threats. - Examine the cyber kill chain & the layers of control used to defend against it. - Discuss how pen-testers use adversarial thinking & the cyber kill chain to test defenses. - Identify examples of each stage of the cyber kill chain & brainstorm protective measures. - Visit *Have I Been Pwned* to determine if students' email accounts have been compromised in a breach.

Guiding Questions:

- Who is the adversary?
- What does he want? Why?
- How can he adapt?
- What are the stages of the cyber kill chain?
- How do you defend against these?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
7.2.2 LO: Students will be able to describe how the presence of an adversary necessitates that cybersecurity risk is emergent and complex.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Souppaya, Murugiah and Scarfone, Karen, "Guide to Malware Incident	• Show students the following quote by David Berstein: "For every lock, there is someone out there trying to pick it or break it." Do the students agree or disagree with the quote? Why? • Ask students who they think adversaries are (review from previous units). What do they want? How and when will

7.2.2a EK: Adversaries employ strategic reasoning, including where, when, and how they might attack, as well as tactics for evading detection. 7.2.2c EK: Adversaries are self-interested agents whose behavior evolves and adapts in response to their environments and other actors in the system. 8.1.1g EK: The emergence of advanced persistent threats (APTs) have caused changes in the way individuals and companies are secured and who is involved in securing them. 8.1.1g EK: The emergence of advanced persistent threats (APTs) have caused changes in the way individuals and companies are secured and who is involved in securing them.	Prevention and Handling for Desktops and Laptops." SP 800-83 Rev. 1, *NIST.gov,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf • Cichonski, Millar, Grance, and Scarfone. "Computer Security Incident Handling Guide; Recommendations of the National Institute of Standards and Technology." SP 800-61 Rev. 2, *NIST*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf	he try to get what he wants? The questions are difficult to answer, as the abilities and motives vary. This makes cybersecurity complex. • Discuss how adversaries have strategies and adapt the strategies based on the target system and how it is protected. Have students look for and provide examples of this. • Ask students to list some threats to a system (Denial of Service/ Distributed Denial of Service (DDoS),Man in the Middle (MitM), Social Engineering, Malware and Spyware, Password Attacks, Advanced Persistent Threats (APT). Go over the definition of each of these. The publications linked left can assist in teaching these threats and how experts can respond. • Discuss APTs. How does an entity plan for these advanced persistent threats? • Review the incident response life cycle linked left. Why is this life cycle needed? Students did research on this life cycle in Unit 2. Have students pull from this research to review the concepts with the class.
6.2.3 LO: Students will analyze how the cybersecurity attack lifecycle/kill chain is essential to adversarial thinking.	• "What is the cyber kill chain?" *YouTube*, uploaded by IDG TECHtalk, 12 Feb 2019,	• Examine and overview of the cyber kill chain. Remind students that this is just a model and attacks may not follow this exact path. • Show the video linked left to facilitate discussion.

7.2.2b EK: The steps in an attack are footprinting, scanning, enumeration, network mapping, gaining access, privilege escalation, implant, and hiding tracks.	https://www.youtube.com/watch?v=zhCIg4cLemc • "How the Cyber Kill Chain Can Help You Protect Against Attacks." SBS CyberSecurity, *SBSCyber.com*, 23 Aug 2019, https://sbscyber.com/resources/how-the-cyber-kill-chain-can-help-you-protect-against-attacks	• To protect against the cyber kill chain, an entity should have layers of control. These are: detect, deny, disrupt, degrade, deceive, and contain. Have students examine the source linked left to help students see the correlation between these layers and the kill chain.
6.2.3b: Reconnaissance is the first stage in the attack lifecycle, where adversaries gather public information about the target, and scan their networks to identify how best to plan their attack.	• "Rapid7 Under the Hoodie – The Pizza of Doom." *YouTube*, uploaded by Rapid7, 23 July 2019, https://www.youtube.com/watch?time_continue=2&v=PeO3Qs84GqQ&feature=emb_logo • Breaking the Kill Chain: "Breaking The Kill Chain: A Defensive Approach." *YouTube*, uploaded by The CISO Perspective, 5 Feb 2019,	• Next, have the students watch a series of videos that show penetration testers. Explain to students that, while penetration testers use the same cyber kill-chain to test defenses, they do so legally. This video series allows people to see what a potential attacker could do. They will then discuss what the company should do to protect strengthen their security. • Watch video, "The Pizza of Doom," linked left. Ask students to provide examples of reconnaissance the penetration testers used. They then should brainstorm ways to protect against reconnaissance. • Explain the difference between active and passive reconnaissance. Have students watch the Reconnaissance section of the video linked left ("Breaking the Kill Chain: A

	https://www.youtube.com/watch?v=II91fiUax2g • Cichonski, Millar, Grance, and Scarfone. "Computer Security Incident Handling Guide; Recommendations of the National Institute of Standards and Technology." SP 800-61 Rev. 2, *NIST*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf	Defensive Approach"). Students could also pull from the NIST Incident Response Life Cycle publication linked left to brainstorm defensive strategies for each stage.
6.2.3c: Weaponization is the second stage. Based on the information obtained through reconnaissance, the adversary will tailor their toolset to meet the specific requirements of the target network. This often includes coupling remote access with an exploit into a deliverable payload. 6.2.3d: The third phase is delivery, which is the transmission of the weapon to	• Weaponization: "Rapid 7 Under The Hoodie – You Had Me Before 'Hello'." *YouTube*, uploaded by Rapid7, 8 Feb 2017, https://www.youtube.com/watch?v=uYJPH1nct_U&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=5 • Delivery: "Rapid7 Under The Hoodie – Pwned You	• Repeat this process for the rest of the stages of the kill chain. For each stage, explain the concept, have students look for examples in the video and brainstorm protective measures, and then show the correct segment of "Breaking the Kill Chain: A Defensive Approach" to learn best practices regarding the stage. • Note that another step by attackers is often to hide their tracks. Have students investigate ways to do this. Did they see any examples of this in the videos? • Have students visit the Have I Been Pwned website. Here, they can check to see if any of their email accounts have ever been compromised. If any have, ask students if they

the target environment using vectors like email attachments, phishing, websites, and removable media. 6.2.3e: Exploitation is the fourth phase where the code is triggered exploiting vulnerable applications or systems. 6.2.3f: The fifth stage is installation where attackers install a remote access trojan or backdoor on the victim system in order to conduct further operations, such as maintaining access, persistence and escalating privileges. 6.2.3g: Command and control is the sixth phase of the cyber kill chain. With malware installed, attackers now own both sides of the connection: their malicious infrastructure and the infected machine and can now actively control the system. Attackers will establish a command channel in order to communicate and pass data back and forth between the	Twice." *YouTube*, uploaded by Rapid7 8 Feb 2017, https://www.youtube.com/watch?v=QMAJ4bVB3EI&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=4 • Exploitation: "Rapid7 Under The Hoodie – One Man's Junk Is Another Man's Treasure." *YouTube*, uploaded by Rapid7, 8 Feb 2017, https://www.youtube.com/watch?v=QHPSfHsgIEc&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=3 • Installation: "Rapid7 Under The Hoodie – The Cardboard Box." *YouTube*, uploaded by Rapid7, 23 July 2019, https://www.youtube.com/watch?v=gVj-ELJz5u8&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=9	were notified of the breach. Have they changed their password since the breach occurred?

infected devices and their own infrastructure. 6.2.3h: The final stage of the kill chain is actions on the objective. Once adversaries have control, persistence, and ongoing command and communication, they will act upon their motivation in order to achieve their goal(s), e.g., data exfiltration, destruction of critical infrastructure, to deface web property, or to create fear or the means for extortion.	• Command and Control: "Rapid7 Under The Hoodie – Remote Control." *YouTube*, uploaded by Rapid7, 8 Feb 2017, https://www.youtube.com/watch?v=t-yY8sGv4LY&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=2 • Actions on the Objective: "Rapid7 Under The Hoodie – The Bank Job." *YouTube*, uploaded by Rapid7, 8 Feb 2017, https://www.youtube.com/watch?v=_7dj6K4qY7E&list=PLMrgKzfE1aIMaabJsp4vxRmVZ1fJs41XQ&index=1 • *Have I Been Pwned?* https://haveibeenpwned.com/	
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.		• For a career, you could discuss a cyber crime investigator.

UNIT 19: Network Security Technologies

Estimated Time in Hours: 7

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
3 Ubiquitous Connectivity 6 Adversarial Thinking 2 Establishing Trust	3.2	- Investigate firewalls, Intrusion Detection Systems, Intrusion Protections Systems, Application Layer Defenses, and IoT Defenses. - Research Types of threat indicators (pyramid of pain). - Provide a defense in depth network model.

Guiding Questions:

- Why are network security technologies needed?
- What are these technologies?
- What are the types/features of these technologies?
- How/why is security a characteristic of a system, not a tool?
- Why is layering (defense in depth) important?
- What happens when the tools fail?
- What is the role of policy?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
3.2.3 LO: Students will identify and distinguish between the purposes of network security devices and technologies. 3.2.3a EK: Most protocols lack a security component but some protocols build in security. For example, http was designed before security was a major concern while extensions like	• Computer, lecture slides, projector, graphic organizers, access to Internet • Timberg, Craig. "Net of Insecurity Part 1 | A Flaw in the Design | The real story of how the Internet became so vulnerable." The Washington Post,	"The Internet is not the setting of most attacks. It is the delivery system."– Craig Timberg • Ask students if they agree or disagree with the quote. Explain how the Internet was originally designed for information sharing; therefore, security was not a concern. It was built for speed and ease. Use http/https as an example here. • Note that the Internet was made with a dumb core that was designed to carry data to intelligent edges (individual computers). Review how packets are carried across the

https explicitly add security to the standard. 3.2.3b EK: A packet can be identified by its source address (sending device), source port (sending application on the device), destination address (receiving device), and destination port (receiving application on the device).	*WasingtonPost.com*, 30 May 2015, https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?utm_term=.ba1761c56b14	dumb core to the intelligent edges. The article linked left can help with these concepts.
3.2.3c EK: Firewalls work primarily at the network and transport layer by blocking packets with addresses and ports that correspond to unwanted traffic.	• "What are Firewalls?" *YouTube*, uploaded by CBT Nuggets, 31 Jan 2019, https://www.youtube.com/watch?v=9JQtyQEpQV8 (7:58 minutes) • "Security in Formation | 5 Generations of Firewall Solutions." CypherShark, *Sharkscale.WordPress.com*, 7 May 2016, https://sharkscale.wordpress.com/2016/05/07/5-generations-of-firewall-solutions/ • Souppaya, Murugiah and Scarfone, Karen, "Guide to Malware Incident	• List types of network security technologies designed to secure a system (the intelligent edges). These should include firewalls, intrusion detections systems, intrusion protection systems, application layer defenses, and IoT defenses • Provide an overview of a firewall. Explain its role in a security system. Show video linked left. • Discuss firewall types. See source linked left. • Discuss firewall placement (host-based, network based, cloud-based). Have students research the pros and cons of each type. • Discuss firewall rules. The NIST publication linked left offers resources for this on page 13. NIST also offers *Guidelines on Firewalls and Firewall Policy*, also linked left.

	Prevention and Handling for Desktops and Laptops." SP 800-83 Rev. 1, *NIST.gov,* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf (See page 13) • Scarfone, Karen and Hoffman, Paul. "Guidelines on Firewalls and Firewall Policy." SP 800-41 Rev. 1, *NIST.gov*, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf • Sehl, Sibylle and Vaniea, Kami. "Unity WebGL Player | SecondGameDraft." The University of Edinburgh School of Informatics, https://groups.inf.ed.ac.uk/tulips/projects/1617/PermissionImpossible/	• Use the game linked left to allow students to practice firewall rules.
3.2.3d EK: Intrusion Detection Systems (IDS) work at all layers to identify and raise an alarm when	• "Zero Day Exploit explained under 2 mins." *YouTube*, uploaded by	• Show video linked left. Have students define a zero-day attack in their own words. Explain to students that entities

unexpected message patterns (anomalies) or known bad patterns (signatures) are detected (blacklisting). IDS systems can also be configured to block all packets and only allow a select set of valid packets (whitelisting). 3.2.3e EK: Intrusion Prevention Systems (IPS) are similar to IDS and also can prevent attacks by blocking messages related to anomalies or signatures.	Cyber Security Entertainment, 26 Dec 2017, https://www.youtube.com/watch?v=PNgIJXodwic • Slowik, Joe. "Unraveling Detection Methodologies: Indicators vs. Anomalies vs. Behaviors." *RSA Conference 2019 | San Francisco | March 4-8 2019*, https://published-prd.lanyonevents.com/published/rsaus19/sessionsFiles/13770/AIR-T09-Unraveling-Detection-Methodologies-Indicators-vs.-Anomalies-vs.-Behaviors.pdf • "The Pyramid of Pain." Enterprise Detection & Response, http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html	have to worry about all kinds of attacks, especially zero-day attacks. How do they protect against them? • Discuss the definition of an IDS. Discuss whitelisting and blacklisting. Discuss the types of IDSs (signature detection, anomaly detection, behavior-based). The slideshow linked left is a good resource to explain the differences. • Have students research types of indicators using the site linked on the left (Pyramid of Pain). Discuss HIDS versus NIDS. • Introduce IPS and contrast to IDS. Show video linked left.

	• "MicroNugget: IDS vs. ISPs." *YouTube*, uploaded by CBT Nuggets, 16 Jan 2014, https://www.youtube.com/watch?v=rvKQtRklwQ4	
3.2.3f EK: Application layer defenses, such as input validation, check and block potentially harmful message data from getting to the application. 3.2.3g EK: Devices with limited processing power such as Internet of Things (IoT) devices and control systems in industrial settings may rely almost entirely on network security devices such as firewalls and IPS for protection.	• "Input Validation Cheat Sheet." OWASP Cheat Sheet Series, Open Web Application Security Project, *OWASP.org*, https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html • "OWASP Top Ten Proactive Controls 2018 | C5: Validate All Inputs." Open Web Application Security Project, *OWASP.org*, https://owasp.org/www-project-proactive-controls/v3/en/c5-validate-inputs • "Defense-in-Depth. Layered Protection and Data Security." Infosec Institute, *InfosecInstitute.com*, 28 Sep 2014,	• Discuss application layer defenses. The sites linked left can assist with this. The video linked left also show an example of the importance of input validation and has an activity to go with it (see left). WARNING: The video has bleeped language. Please preview before showing. • Discuss how IoT devices have very little built in security. This means they have to depend on the security of the network. The article linked left is useful for teaching this this.

	https://resources.infosecinstitute.com/defense-depth-layered-protection-data-security/#gref • "Hacking Websites With Cross-Site Scripting (XSS Attack Basics)." *YouTube*, uploaded by Chef Secure, 2 Nov 2018, https://www.youtube.com/watch?v=9kaihe5m3Lk • "Hacking Websites With Cross-Site Scripting." *ChefSecure.com*, https://chefsecure.com/courses/xss/recipes/hacking-websites-with-cross-site-scripting • Craven, Connor. "What is Edge Security? Definition." SDxCentral, *SDxCentral.com*, 27 Mar 2020, https://www.sdxcentral.com/edge/definitions/what-is-edge-security-definition/	

6.1.2e EK: Security is a characteristic of systems and not system components. 2.3.5 LO: Students will break down how the principle of layering is a strategy for slowing down an attack because the attacker has to conquer each layer before moving on to the next. 2.3.5a EK: A layer is a separate level that must be conquered by an attacker to breach a system. 2.3.5b EK: Multiple independent layers require integration and independent management to get the full benefits of layered protection.	• "How the Cyber Kill Chain Can Help You Protect Against Attacks." SBS CyberSecurity, *SBSCyber.com*, 23 Aug 2019, https://sbscyber.com/resources/how-the-cyber-kill-chain-can-help-you-protect-against-attacks	• Ask students to explain how security is a characteristic, not a tool. Discuss how the tools have to be properly configured to provide security. • Have students examine the matrix linked left. What weapons are in place to protect a system from each stage of the cyber kill chain? How is layering used? Have students link these strategies with security technologies on a network.
6.1.2 LO: Students will explain how complexity impacts the failure of cybersystems. 6.1.2c EK: Product failure is deceptively difficult to understand given that it depends on the intrinsic properties of each part, what it's made of, how those materials respond to		• Ask if any of these devices could fail. If so, what would happen? • Discuss unified threat management (UTM). Is it a good or bad idea? Have students explain. Discuss redundancy. • Have students research examples of the times system failures have resulted in a breach.

varying and unanticipated conditions, and how customers use a product. 6.1.2a EK: In complex systems, failures are rarely the result of one individual's problem or behavior; catastrophe requires multiple failures. 6.1.2b EK: System failures are characterized by a series of actions or behaviors that are normally isolated or self-contained, but become consequential due to interconnected impact. 6.1.2d EK: Given the complexity of cybersystems, there are limits to how much entities can control their functioning and success of their policies.		• Have students create a network diagram for a fictitious company. They should include network devices to protect against malicious software, phishing, spam, leakage of intellectual property, BYOD, and rogue access points. The technology should not be limited to the ones discussed in this unit. Have students explain their choice and include these items in their network diagram. • Note the importance of user training and auditing.
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.		• Discuss a career. We recommend a career as a warnings analyst.

UNIT 20: Network Meets Cryptography

Estimated Time in Hours: 5

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 7 Risk		- Use *traceroute* to discover the number of devices between their computer and a destination website. - Check the domain of the discovered IP addresses to find out who owns them. - Use Wireshark to view plaintext network traffic on non-HTTPS websites. - Make a case for or against the security of the Internet.

Guiding Questions:

- Where does your network traffic go after it leaves your computer? How can you track this?
- Who can see encrypted web traffic?
- Who can see unencrypted web traffic?
- Which parts of the CIA Triad can man-in-the-middle attacks violate?
- How does cryptography protect information on untrusted networks?
- What is the role of certificate authorities?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
7.2.4 LO: Students will be able to explain how the decentralized and dynamic nature of networked systems create the potential for a system to fail or behave incorrectly due a component the designer didn't even know existed.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Windows *tracert* command, access to http://www.arin.net/whois/ , and a tutorial like:	• Ask students where their network traffic goes when they browser to a website. The obvious answer is to the website destination; however, where does it go in-between? • Explain that the Internet is built to facilitate communication. Security has become increasingly important, but it's not always there, and there's plenty of adversaries trying to steal your data.

7.2.4a EK: There are risks and mitigations associated with open systems like the Internet. 7.2.4b EK: Internet communication between a sender and receive relies on a number of systems that are not controlled by the sender or receiver. This can include the hardware and software at the sender and the sender's edge network. It includes a number of supporting systems such as the DNS and certificate authorities, and any number of intermediate networks. It can also include the receiver's edge network as well as the hardware and software at the receiver.	"Lab 1.2.3 Mapping ISP Connectivity Using Traceroute." Cisco | Networking Academy, https://web.nmsu.edu/~jbeasley/Cisco_Discovery_4-1/courses/en0500000000/en0501000000/en0501020000/en0501020300/en0501020303/cm6042232704/lab.pdf	• Let students experience this first-hand using *traceroute* to identify the computers between their system and a destination website.
7.2.4c EK: Incorrect assumptions about the network can result in the loss of confidentiality by sending data to an imposter or sending data over a path where it can be observed.	• Wireshark and access to non-HTTPS website. Lists of these can be found online; however, they are becoming more rare to find – this is a good thing. Websites with unencrypted images make for an excellent use case as students can find	• Explain the dangers of sending traffic over insecure connections. • Have students use Wireshark to visit non-HTTPS websites and observe the plaintext traffic. • Explain or review man-in-the-middle attacks as another method to snoop on traffic.

	the links to those pictures in Wireshark. • Man-in-the-Middle Attack overview: "What Is a Man-in-the-Middle Attack?" *YouTube*, uploaded by Hacksplaining, 4 Mar 2017, https://www.youtube.com/watch?v=DgqID9k83oQ	
7.2.4d EK: Network vulnerabilities can result in the loss of integrity if data is sent to an imposter acting as a "monkey-in-the-middle" or when data is sent over a path where it can be changed.		• Ask students if the man-in-the-middle attack can be used other ways. • A man-in-the-middle who can intercept all web traffic from the victim can then change the traffic mid-transit to violate the integrity.
7.2.4e EK: Network vulnerabilities can result in the loss of availability by directing the sender to an invalid destination or sending data over a path where it can be dropped.	• Man-in-the-Middle availability attack against a drone: "DoS by man-in-the-middle attack." *YouTube*, uploaded by Mehdi Karimi, 3 Mar 2019, https://youtu.be/SrJvO4RwMUQ	• If an adversary can view and alter traffic, what else can they do? They can drop traffic and prevent it from reaching its destination. • Ask students which parts of the CIA Triad a man-in-the-middle attack violates.

7.2.4f EK: Cryptography can be used to prevent imposters and protect data so only authorized entities can view it. 7.2.4g EK: Cryptography can be used to identify the creator of a message and show a message was not modified in transit (hash function).		• Ask students the best way to protect themselves when using the Internet. • Cryptography is the best solution as it prevents any parties in the middle from viewing data. • Asymmetric cryptography can also provide integrity and authentication to prevent man-in-the-middle attacks. • Review protocols secured with cryptography.
7.2.4h EK: Certificate authorities play a role in asserting the identities.	• Certificate Authority explanation and demonstration in the face of man-in-the-middle attacks: Challen, Geoffrey. "What is a certificate authority?" *YouTube*, uploaded by internet-class, 17 Oct 2016, https://youtu.be/8ItJ-VqYo_s	• Review Certificate Authorities as the trusted third-parties who ensure communications are secure. • Explain the importance of a certificate and why they must be legitimized by a certificate authority. • Show the linked YouTube video and use a video viewing guide to assess learning. • Ask students what would happen if a certificate authority was compromised?
7.2.4i EK: Cryptography does not solve operational challenges and cryptography alone is not a solution in a decentralized network.		• Review that cryptography is an important piece of the solution, but not necessarily a catch-all. • The environment's security (e.g., CAs, PKIs) is also paramount.
2.3.6 LO: Students will know that the principle of data hiding is		• Review the principle of data hiding.

about allowing only necessary aspects of a data structure or a record to be observed or accessed. 2.3.6a EK: Data hiding can help prevent users/programmers/processes from updating/changing data in invalid ways or by mistake.		• Ask students to describe how data hiding applies to man-in-the-middle attacks. • Ask students to explain how data hiding applies to certificate authorities. • As an independent assignment, task students with making a case for whether or not the Internet is secure. How can they back up this claim?
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 operator.

UNIT 21: Hardware & Software Integration

Estimated Time in Hours: 10

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
5 System Security 2 Establishing Trust	5.1	- Demonstrate knowledge of both software and hardware by writing a simple python program to blink an LED on a computer-connected breadboard. - Research how internal and external hardware interacts with software. - Research types of malware and hardware vulnerabilities.

Guiding Questions:

- Does hardware depend on software for computing?
- Without hardware, how does software work?
- How does internal and external hardware interact with software?
- What are the categories of malware?
- Does hardware matter for malware?
- What is the difference between low level and high level programming languages?
- What does a software engineer need to consider when developing software for a specific hardware platform?
- How does domain separation relate to hardware and software?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
5.1 EU: Systems consist of a combination of hardware and software that together achieve some objective and security requires integration of both. 5.1.1 LO: Students will identify how hardware and software	• Computer, lecture slides, projector, graphic organizers, access to Internet • How hardware and software work together: "How Computers Work: Hardware and Software."	• Show the YouTube video and use a video viewing guide to assess learning. • Ask students how hardware and software work together.

work together in complex ways to achieve an overall objective.	*YouTube*, uploaded by Code.org, 30 Jan 2018, https://youtu.be/xnyFYiK2rSY	
5.1.1b EK: Neither hardware or software is useful without the other. 5.1.1e EK: Software includes programs written to run on servers, laptops, and traditional computers. Computing devices accomplish no tasks without running software that tells it what to do.	• Examples of hardware and software and how they require each other: "Computer Science Basics: Hardware and Software." *YouTube*, uploaded by GCFLearnFree.org, 3 Oct 2018, https://youtu.be/vG_qmtdBPTU	• Explain that a computer must consist of both hardware and software. • Ask students to explain what their phone could do without any software. • Show the linked YouTube video to emphasize that without software, the computer is just a pile of electronics. Without hardware, the software instructions will not achieve any results. • Task students with providing concrete examples of software and hardware working together.
5.1.1c EK: Software instructions may manipulate data, manipulate physical systems or manipulate both. For example, software in a vehicle may record the vehicle speed and send it to a cloud storage system, other software may cause the brakes to be physically applied and reduce the speed, and still other	• How software interacts with hardware, and vice-versa: Bair, Bettina. "Inside your computer." *YouTube*, uploaded by TED-Ed, 1 July 2013, https://youtu.be/AkFi90lZmXA	• Explain the details of how software interacts with hardware. • Show the linked YouTube video and review how the instructions from a mouse interacts with software and hardware again. Use a video viewing guide if necessary. • Optionally, use hardware/build a PC graphic organizers from Unit 3 here. Task students with classifying how internal and external hardware interact with software. This can be a research project.

software may both record and manipulate the vehicle speed.		
5.1.1d EK: Malware, short for malicious software, is any software intentionally designed to cause damage to a computer, server, client, or computer network.	• Malware overview and categories: "Malware: Difference Between Computer Viruses, Worms and Trojans." *YouTube*, uploaded by Kaspersky, 21 Mar 2016, https://youtu.be/n8mbzU0X2nQ	• Revisit malware and dive into the different categories: virus, worm, botnet, etc. • Ask students how malware impacts hardware. • Assign students a type of malware to research. They should summarize how it infects, its goals, and some examples or implementation of the malware.
5.1.1f EK: Software can be written in high level languages such as Python, C, Perl, Java and the high level software is converted into low level instructions that tell the CPU, memory, and other devices exactly what to do.	• Example software-hardware integration program: "Making a LED blink using the Raspberry Pi and Python." *RaspberryPiHQ.com*, 11 Jan 2018, https://raspberrypihq.com/making-a-led-blink-using-the-raspberry-pi-and-python/	• Describe high level programming languages. • Compare and contrast popular languages. • Challenge students by having them write a simple program in Python to blink an LED wired to a computer-connected breadboard. This lab will demonstrate how software can interact with hardware.
5.1.1g EK: Software can be written in low level machine specific instructions that tell the CPU, memory, and other devices		• Explain low level languages and compare and contrast with high level languages. Point out their advantages and disadvantages.

exactly what to do (e.g. add memory locations one and two and store the result in memory location.		• Show the students examples of each. Ask them which language they would prefer to use to develop software. Why?
5.1.1i EK: Embedded software is computer software, written to control machines or devices that are not typically thought of as computers, commonly known as embedded systems. 5.1.1h EK: Embedded software can be built directly into the physical device so the instructions on how a device will behave are physically part of the device and often cannot be changed without changing the hardware itself.		• Introduce the concept of embedded systems alongside examples and use cases. • Explain how sometimes the hardware and software are tightly integrated in embedded software. • Provide examples of embedded software. Explain how this is similar to an operating system and provides unique optimizations. • Ask students to explain any drawbacks of embedded software.
5.1.1j EK: Software ultimately relies on the physical hardware to accomplish its task and even if the software is written perfectly, it will not perform the desired function if the hardware fails to behave as expected. In other words, the software may correctly instruct the hardware to add two numbers and store the result in memory location 3. If memory location 3 has an error		• Revisit how hardware and software depend on each other to properly compute. • Ask students: in the case of a desktop computer, what happens if the hard-drive fails? What happens if the power supply fails? What happens if the fans fail?

or vulnerability and does not store the correct value, the software will not accomplish its objective.		
5.1.1k EK: Hardware ultimately relies on the software instructions to accomplish its task and even if the hardware operates perfectly, it will not perform the desired function if the software fails directs it to execute the wrong instructions. In other words, the hardware may be able to correctly apply the brakes in a vehicle when instructed to do but it will not prevent a vehicle crash if the software is too slow in deciding when to apply the brakes.		• Conversely, what happens if software fails? What happens your web browser crashes? What happens your operating system fails? • Ask students if they think hardware designers need to be aware of software. Do software designers need to be aware of hardware?
5.1.1l EK: The overall system can be manipulated to act incorrectly if there is a vulnerability in the hardware, the software, the interface between them, or any combination of those.	• Review of Spectre and Meltdown: "Meltdown & Spectre vulnerabilities – Simply Explained." *YouTube*, uploaded by Simply Explained, 15 Jan 2018, https://youtu.be/bs0xswK0eZk	• Review hardware vulnerabilities like Spectre and Meltdown. • Ask students if hardware vulnerabilities are easier or harder to detect than software vulnerabilities. • Have students research specific hardware vulnerabilities. What does it do? How long was the vulnerability in existence before it was discovered? Is there a patch for the vulnerability, and what does it require?

2.3.1 LO: Students will give examples of the principle of domain separation, which allows for the enforcement of rules governing the entry and use of domains by entities outside the domain. 2.3.1a EK: A domain refers to a collection of data or instructions that warrant protection. 2.3.1b EK: Communications between domains are allowed only as authorized.		• Review the principle of domain separation. • Ask students to explain how domain separation deals with software and hardware. • Are software and hardware domains? When should they remain separate, and how should they be used in tandem?
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 information systems security developer.

UNIT 22: Common Hardware Vulnerabilities

Estimated Time in Hours: 8

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
5 System Security 7 Risk 2 Establishing Trust		- Research, identify, and categorize common hardware vulnerabilities. - Research tactics for securing hardware vulnerabilities and supply chain threats. - Develop a physical security plan for vulnerable hardware.

Guiding Questions:

- How does a hardware vulnerability differ from a software vulnerability?
- What are some methods used by adversaries exploiting hardware?
- What is the Meltdown vulnerability and how many computers does it affect?
- What are the types of side channel attacks and how do they differ?
- How do hardware vulnerabilities sometimes involve software?
- How can physical security help protect potentially vulnerable hardware?
- How does resource encapsulation benefit hardware?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
5.2.2 LO: Students will know some common hardware-related vulnerabilities.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Spectre & Meltdown review: "Why are Spectre and Meltdown So Dangerous?" *YouTube*, uploaded by Techquickie, 1 May 2018,	• Review hardware vulnerabilities covered so far (Spectre, Meltdown, physical security vulnerabilities, etc.) • Watch the Spectre & Meltdown review YouTube video. Is there any drawback to mitigating a processor against Meltdown? • Ask students if they think hardware vulnerabilities are easier for adversaries to exploit than software vulnerabilities? Are they easier to detect?

	https://youtu.be/NArwG6yaWJ8 • Common hardware vulnerabilities: Biryukov, Vladislav. "Deep Dive: 5 Threats Affecting Hardware." Kaspersky Daily, *Kaspersky.com*, 1 Apr 2015, https://www.kaspersky.com/blog/hardware-malware/8169/	• Challenge students with researching common hardware vulnerabilities and listing their name, vulnerability, method of exploitation, and any mitigations or fixes. An example link is provided.
5.2.2a EK: A backdoor is a method, often secret, of bypassing normal authentication or encryption in a computer system, a product, or an embedded device (e.g. a home router) to secure remote access. 5.2.2b EK: Manufacturing backdoors are used for malware or other penetrative purposes; backdoors aren't limited to software and hardware, but they also affect embedded radio-frequency identification (RFID) chips and memory.	• Cold boot attack demo: "The Chilling Reality of Cold Boot Attacks." *YouTube*, uploaded by F-Secure, 13 Sep 2018, https://youtu.be/E6gzVVjW4yY • Cold boot attack explanation: "Cold Boot Attack | University of South Wales VeraCrypt Research Group." *YouTube*, uploaded by Luke Clarke, https://youtu.be/XfUlRsE3ymQ	• Explain how many hardware vulnerabilities require backdoor access, many of which are obscure. Provide examples. • Show the linked YouTube video of the cold boot attack. Is this an example of a backdoor? What does the adversary need access to in order to do this attack? • Ask students why adversaries would adversaries be interested in gaining access to the content of memory or RFID cards.

7.2.3d EK: Hardware itself may act in unintended ways and an adversary is seeking to find and exploit these unintended behaviors.		• As demonstrated, adversaries can find unique methods for exploiting unintended hardware behaviors. What is the skill level of hackers who do this? • Ask students to summarize how the cold boot attack works.
5.2.2c EK: A side channel attack is based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs)	• Mobile device side channel leakage: "Side-Channel Analysis Demo: Mobile Device." *YouTube*, uploaded by Rambus Inc., 25 june 2013, https://youtu.be/cPDDNVKo43w • Side Channel Timing Attack demo (technical): "Side Channel Timing Attack Demonstration." *YouTube*, uploaded by Joe Grand, 26 Sep 2017, https://youtu.be/2-zQp26nbY8	• Define the term side channel attack/analysis. Ask students what is the meaning of side channel? • Show the linked YouTube video about the Side Channel Timing Attack. Use a video viewing guide if necessary. What is the purpose of measuring the time of button presses?
5.2.2d EK: General classes of side channel attacks include attacks such as: timing attacks, power-monitoring attacks, electromagnetic attacks, data remanence attacks.		• Define and categorize the types of side channel attacks with examples. • Emphasize that timing attacks are only one type of side channel attack. What type is the cold boot attack shown earlier?

		• Ask students why an understanding of low level hardware, binary, and programming languages is important for side channel analysis.
5.2.2e EK: Hardware vulnerabilities can also be due to weaknesses in the implementation of algorithms.		• Explain that sometimes hardware is expected to be used one way, but software may attempt to use it in another way. This muddies the water between whether the vulnerability is a software or hardware vulnerability. For example, the Meltdown vulnerability is achieved through its branch prediction feature designed to speed up processing; however, the algorithm used is exploitable by adversaries.
5.2.3 LO: Students will describe the process of developing secure hardware and validating that it is secure through its lifecycle. 5.2.3a EK: Hardware itself consists of many components and supply chain management attempts to ensure each component as well as the composition of these components meets an overall security policy. 5.2.3b EK: The hardware design, manufacturing and supply chain can be attacked by malicious actors, nation states,	• Supply chain introduction: "What is Supply Chain Management?" *YouTube*, uploaded by BYU Supply Chain, 5 Jan 2014, https://youtu.be/AwemFfdD6VI • Huawei national security concern: "Why The US Thinks Huawei Is A National Security Threat." *YouTube*, uploaded by CNBC, 24 Dec 2018, https://youtu.be/3l20G4OfGk0	• Hardware and software should be tested together to help prevent exploitation; however, hardware isn't always so simple to protect. • Define the term supply chain and show the introductory YouTube video on the left. The Huawei espionage allegations video can also be shown to promote supply chain discussion. • Ask students how they can trust the origin of hardware. Does the origin of all hardware need to be scrutinized? How can the supply chain be secured?

competitors, and organized crime.		
5.2.4 LO: Students will identify hardware security addresses issues related to an adversary physically gaining access to a device. 5.2.3c EK: Physical security measures can be used to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm.	• Securing supply chain resource: Saleh, Emile and Rizvi, Sarah. "10 ways to secure supply chains." *ITP.net*, 2 May 2020, https://www.itp.net/news/92310-10-ways-to-secure-supply-chains	• Sometimes hardware vulnerabilities cannot be eliminated, but physical security can prevent adversaries from getting their hands on your hardware in the first place. • Review physical security practices from Unit 9. • Task students with developing a physical security plan for vulnerable hardware.
5.2.4a EK: The hardware design can require the device disable itself if physically tampered. 5.2.4b EK: Students will identify examples of fail-safe in cybersecurity, i.e., a design feature or practice that in the event of a specific type of failure, inherently responds in a way that will cause no or minimal harm to other equipment, the environment or to people and provide recovery opportunities.		• Review the concept of failing securely. Does this promote the confidentiality or availability portion of CIA Triad? Which is more important when only information is involved? • It's important to note that in mechanisms and systems which impact people, protection of life should be considered priority in fail-safe design.
2.3.3 LO: Students will explain the importance of encapsulating		• Review the principle of resource encapsulation.

resources, i.e., creating well-defined interfaces around resources to set rules for how the resources should interact. 2.3.3a EK: Examples of resources are the memory, disk drive, network bandwidth, battery power, and a monitor. It can also be system objects such as shared memory or a linked list data structure. 2.3.3b EK: Encapsulation allows access or manipulation of the class data in only the ways the designer intended.		• Ask students to explain how hardware security can benefit from resource encapsulation. • Does the Meltdown vulnerability benefit from a breach in encapsulation? How?
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 system testing and evaluation specialist.

UNIT 23: Conducting Security Testing & Assessments

Estimated Time in Hours: 12

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
7 Risk 1 Ethics 6 Adversarial Thinking	6.2	- Investigate common security testing tools.

Guiding Questions:

- Why are security testing and assessments important?
- What forces threaten security?
- How are security resources allocated?
- What are common security testing tools?
- How can they be abused?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
6.2 EU: Adversarial thinking is the process of reasoning about how opposing forces could prevent a system from meeting both its functional and security goals. 6.2.1 LO: Students will know how natural events and unintentional errors can cause a system to fail. 6.2.1a EK: Cyber systems are susceptible to disruption and destruction from natural disasters; for example, flooding, earthquakes, and hurricanes.	• Computer, lecture slides, projector, graphic organizers, access to Internet • "6 Scenarios for Business Continuity Plan Testing." Agility Recovery, *AgilityRecovery.com*, 16 Sep 2019, https://www.agilityrecovery.com/7-scenarios-for-business-continuity-plan-testing/	• Failing to plan is planning to fail. Have students explain this saying. • Give students an ABC brainstorm page. Using it, they should list all the things, starting with each letter of the alphabet, that can damage a system. Examples: A = adversary, B = botnet, C = criminals. Students can work together if you wish. Have them share their answers. Did any of them list natural disasters? • List types of natural disasters on the board. Have students brainstorm ways each can harm a system. How do these disruptions impact confidentiality, integrity, and availability?

6.2.1b EK: Disaster planning includes provisioning for the confidentiality, integrity and availability of cyber systems during natural disasters. 6.2.1c EK: Disaster planning includes prevention, detection, and response and recovery. 6.2.1d EK: Natural event and unintentional errors typically do not adapt in response to defenses.		• Explain to students that cybersecurity experts have to plan for natural disasters as well as other threats to a system. This is called disaster planning. Disaster planning includes prevention, detection, and response to recovery. Stress that human life should always be a priority. • Discuss the need for business continuity plans. These outline how an organization stays operational during a disruption. Disaster recovery outlines how a business will get up and running after a disaster (typically another location). The source linked left can assist with this. If time allows, have students examine sample business continuity plans and disaster recovery plans. Templates for these are freely available on various websites.
7.1.5 LO: Students will understand the trade-offs between cybersecurity benefits and the total cost of cybersecurity protections. 7.1.5a EK: The outcome of a risk assessment should prioritize what needs to be remediated. 7.1.5b EK: If the data or resources cost less or are of less value than their protection,	• "Choosing a Higher Level of Assurance." *YouTube*, uploaded by KirkpatrickPrice, 18 July 2019, https://www.youtube.com/watch?time_continue=8&v=Sfawv5dP8TQ&feature=emb_logo	• Show students a picture of an inexpensive television. Tell students that an attacker plans to steal the television. How could they protect it? After students strategize, have them come up with the cost of protecting the television. Did the cost of securing it exceed the cost of the asset? If so, is protecting it a good idea? • Stress to students that assets can also have value that exceeds the cost of the technology. For example, data stored on a laptop may be worth thousands (or even millions) of dollars. That data would merit protecting the laptop.

adding security mechanisms is not cost effective. 7.1.5c EK: The level of protection is a function of the attack occurring and the effects of the attack should it succeed.		• Risk management is risk identification, risk assessment, and risk control. • Review risk assessments with students (see previous units). Remind students that risk assessments help determine what kind of controls show be in place. • Audits determine if controls exist (compliance) and if they are functioning to an acceptable level (adequacy). Explain that there are many types of audits (IS, compliance, financial, operational, integrated, administrative, specialized, computer forensic, and functional. The short video linked left gives a brief overview of an audit.
7.1.4 LO: Students will be able to conduct standard security testing and assessments. 7.1.4a EK: Vulnerability assessment identifies known vulnerabilities on the system. 7.1.4b EK: Known vulnerabilities can be found in databases that collect, maintain, and disseminate information. 7.1.4c EK: There are various automated vulnerability scanning tools, which are used for pinpointing vulnerabilities and	• Barnett, Patrick. "Vulnerability Scanning vs. Penetration Testing." Secureworks, *Secureworks.com*, 20 Dec 2017, https://www.secureworks.com/blog/vulnerability-scanning-vs-penetration-testing • Network Scanners: ○ ipconfig/ifconfig/ip (cmd) ○ ping and arp (cmd) ○ nmap (tool) • Service Discovery: ○ netstat (cmd)	• Explain to students that there are different types and scopes of security assessments. However, most require reconnaissance, security posture assessment, vulnerability scanning or penetration testing, and interviewing. • Note that vulnerabilities can be found in databases that collect, maintain, and distribute information. Have students list examples of these databases. • Note that vulnerability tests can be found using tools. Review/cover these tools (network scanners, DNS harvesting, fingerprinting/sniffing software, wireless scanner/crackers). Discuss passive versus active scanning and false positives/false negatives. Also note that scans can be credentialed or non-credentialed. See list to the left. The source linked to the left also provides notes and further resources. **It is up to the teacher to determine the**

providing remediation for these vulnerabilities. 7.1.4d EK: Not all vulnerabilities can be exploited and not all vulnerabilities need to be mitigated. 7.1.4e EK: Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.	○ nmap (tool) • Fingerprinting: ○ nmap (tool) ○ traceroute (cmd) • Banner/OUI Grabbing ○ nmap • Sniffer & Protocol Analyzers ○ Wireshark • Nadhori, Isbat Uzzin. "Modul 2 | Footprinting Scanning Enumeration." Insitut Teknologl Sepuluh (ITS), https://studylib.net/doc/9262668/modul-2---footprinting-scanning-enumeration • Site: "Onine Banking Login." Altoro Mutual (test website published by IBM), http://www.testfire.net/login.jsp • Web Application Report: https://www.ibm.com/developerworks/community/blogs/48a78681-82cc-434f-9c78-	**maturity of the student in introducing these resources. Teachers should work with their school's IT team before having students use these tools on a school's system.** • Introduce honeypots and honeynets. Note that they assist in identifying and analyzing attacks and act as decoys. • Ask students if all vulnerabilities can be exploited. Why not? Ask students if all vulnerabilities need to be mitigated. Why not? • Define the term penetration test. Have students do a Venn diagram comparing/contrasting a vulnerability scan to a penetration test. Students can use the source linked left to help with this. • Note that before doing a penetration test, a pen tester should obtain written consent from the company and any related vendors, such as the Internet service provider. Additionally, the pen tester should outline the rules of engagement. This includes defining the perimeter, any restrictions, the attack profile (black, white, gray), the environment and timing, how to disclose results, and confidentiality requirements. Pen testers should understand that the legality of pen testing varies from country-to-country and may require end user warning or other documentation. • Pen testing includes reconnaissance (open source intelligence, social engineering, and scanning), initial

	3e9117bfd466/resource/demo.testfire.netSecurityReport.pdf?lang=en • Solutions: "How to hack www.testfire.net." *LSABlog.com*, 21 May 2017, https://www.lsablog.com/networksec/penetration/how-to-hack-www-testfire-net/	exploitation, persistence, escalation of privilege and pivot, and action on objectives. The site and resources linked left are related to a demonstration of a weak site. **Teachers may allow students to experiment on this site; however, teachers should stress that the skills students practice should be limited to this site and should only be done under supervision. Other sites (hackthissite.org and owasp.org/www-project-webgoat/ also offer avenues for supervised student practice.**
1.2.2b EK: Security tools were designed to help system administrators and users to improve security, but an adversary can use the same tools to exploit the target for nefarious goals.		• Note that the same tools used by network administrators to find weaknesses in a system can also be used by adversaries. Have students brainstorm how this can be the case.
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 career, such as exploitation analyst or IT auditor

UNIT 24: Cyber Physical Systems

Estimated Time in Hours: 9

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
5 System Security 4 Data Security 2 Establishing Trust 8 Implications		- Research the types of CPS in various sectors. - Later, identify vulnerabilities which may affect those CPS. - Replicate a developed IoT system and enhance it with a plan for cybersecurity additions.

Guiding Questions:

- What is a Cyber-Physical System and how is it different from a computer?
- What industries or workforce sectors use CPS?
- How are CPS vulnerable to cyber attack?
- What kind of harm can a CPS cyber attack cause?
- What is the benefit of CPS compared to the risk?
- Why is fail-safe design important to CPS?
- How are CPS and Internet of Things intertwined?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
5.4.2a EK: A cyber-physical system (CPS) is a mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users.	• Examples of Cyber-Physical Systems (first minute of the video): "Cyber-Physical Systems | UC BerkeleyX on edX | About Video." *YouTube*, uploaded by edX, 8 May 2014, https://youtu.be/7zSCnnJE1cs	• Define and introduce CPS. This will need to be introduced as a system before adding cyber elements to it. Cover the basics such as actuators, sensors, and human-machine interfaces, and network connections.
5.4.2b EK: Industries that employ CPS include energy management,	• Example of CPS in industry:	• Explain how CPS fits in to various sectors.

health care, manufacturing, transportation, telecommunications, infrastructure, and military.	"Cyber-physical Production Systems." *YouTube*, uploaded by Siemens, 20 June 2018, https://youtu.be/wro3uoHR-ZY • CPS overview with a focus on ethics (prescreen – for a mature class): "The Ethics of Cyber-Physical Systems." *YouTube*, uploaded by MySTOA, 22 May 2016, https://youtu.be/c5gu8xmmum4	• Discuss the implications of integrating CPS into so many industrial. Show the linked CPS overview YouTube video to promote discussion. Are these CPS additions good or bad? What are the repercussions of these changes? Who should be held responsible when CPS fail? • Challenge students with researching the types of CPS in different sectors (energy, health, transit, etc.) to include equipment, efficiencies derived from CPS, and how it improves the goal of the industry.
5.4.2c EK: A smart grid is an electrical grid which includes a variety of operation and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficient resources.	• Smart grid overview: "What is the smart grid? – by Scientific American." *YouTube*, uploaded by Scientific American, 30 Mar 2011, https://youtu.be/-8cM4WfZ_Wg • Power grid cyber attack: Sussman, Bruce. "Revealed: Details of 'First of Its Kind' Disruptive Power Grid Attack." SecureWorld,	• Ask students to explain the advantages and disadvantages of the smart grid. Do you think the smart grid is vulnerable to a cyber attack? • Cyber-physical implies that a cyber attack can have tangible, physical consequences. What kind of harm could a CPS attack cause?

	SecureWorldExpo.com, 8 Oct 2019, https://www.secureworldexpo.com/industry-news/first-u.s.-power-grid-attack-details	
5.4.2 LO: Students will predict how physical systems that rely on software may be vulnerable to future attacks. 5.4.2d EK: Increased industry connectivity will cause increased attacks from adversaries such as cyber criminals, disgruntled employees, terrorists, organized crime, and nation states.		• The benefit of CPS is convenience, efficiency, and safety. The risk is an exploitable system. • Discuss with students why CPS systems may be of particular interest to an adversary. Why might it attract the attention of the most powerful adversaries: nation states?
5.4.2e EK: Vulnerabilities may allow adversaries to interfere with connected devices.		• Delve into specific vulnerabilities of CPS. This can be dependent on the industry, but there is commonality. Most CPS use commercial grade programmable logic controllers and have feedback control with a human machine interface. • Task students with researching CPS vulnerabilities which relate to the CPS in the sector(s) they identified earlier. Are these vulnerabilities dire? Do they have mitigations?

5.4.2f EK: The consequences of unintentional faults or malicious attacks could have severe impact on human lives and the environment.	• Aurora power grid generator attack demo: "Aurora Test Footage." *YouTube*, uploaded by MuckRock, 9 Nov 2016, https://youtu.be/LM8kLaJ2NDU	• Show the linked Aurora demo YouTube video to demonstrate how a cyber attack can destroy a power grid generator. • Ask students to explain the impact of CPS attacks and back it up with reasonable examples. How can they impact hospitals that depend on power?
5.4.2g EK: By targeting trusted resources attackers can control devices and wholeheartedly manipulate users.		• A common CPS attack vector is to gain access to the human machine interface. The CPS can often be controlled from this interface. It also receives sensor feedback data from the devices and is vulnerable to man-in-the-middle attacks. • Ask students what measures they would take to secure trusted resources such as the HMI. Do they need continuous monitoring?
2.3.8 LO: Students will define the principle of fail-safe defaults, which restricts how privileges are initialized when a subject or object is created. 2.3.8a EK: When something does not work or the system fails, the system must return to a secure state. 2.3.8b EK: A secure state is a condition when no subject can access any object in an unauthorized manner		• Review fail-safe defaults and secure states. Why are these important in the context of CPS? • Ask students to explain how to secure CPS from different industrials with fail-safe design. Does the risk of human life play a factor in the design? • Note the trade-offs between availability, confidentiality, and safety. Students should navigate through complex ethical scenarios involving system fail-safe defaults and permissions.

2.3.8c EK: Turning off permission causes a security problem.		
8.1.2d EK: The Internet has evolved to include new types of devices and the "Internet of Things." 8.1.2e EK: The "Internet of Things," benefits our daily lives by providing easier access to information, the ability to offload menial tasks, and coordinate necessary information. 8.1.2f EK: The Internet and IoT devices create new vulnerabilities an adversary can exploit. 8.1.2g EK: The increasing dependence on the Internet and IoT devices introduces problems when these systems become unavailable.	• IoT in manufacturing: "How it Works: The Internet of Things and Manufacturing." *YouTube*, uploaded by IBM Think Academy, 10 Nov 2016, https://youtu.be/R5RfSQ3Nxzg • IoT student design projects: Hasan, Mehedi. "Top 20 Best Internet of Things Projects (IoT Projects) That You can Make Right Now." UbuntuPIT, *UbuntuPIT.com*, https://www.ubuntupit.com/best-internet-of-things-projects-iot-projects-that-you-can-make-right-now/	• Review the Internet of Things. Students should be able to identify IoT devices present in the classroom or at home. • Introduce the future of an expanded CPS network, sometimes called the Industrial Internet of Things or Industrie 4.0. These concepts combine CPS and IoT with machine learning for enhanced efficiency. • Show the linked YouTube video for IoT in manufacturing. What enhancements does IoT bring to the world of CPS? Use a video viewing guide to assess student comprehension. How does this contribute to the complexity of cyberspace? • If resources allow, students can undertake a simple IoT design project. The project can be a recreation of an existing design with an added plan for cybersecurity enhancements. Some ideas are linked to the left.
8.1.1h EK: Cybersecurity events have led to the development of various cybersecurity career paths and various needs in order		• Explore a relevant career, such as cyber intel planner.

to prepare people for these new types of jobs.		

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.