Bastian | Planning & Pacing Guide

Contents

Course Planning and Pacing by Unit

Unit 1: Law and Ethics – Big Ideas 1, 4, 5, 8
Unit 2: CIA Triad – Big Ideas 2, 4, 8
Unit 3: Hardware & Software Basics – Big Ideas 2, 5
Unit 4: Computer System Security (Image Hardening) – Big Ideas 2, 4, 5
Unit 5: Cryptography – Big Ideas 2, 4, 7, 8
Unit 6: Networks, The Internet and IOT – Big Ideas 1, 3, 5, 6, 7, 8
Unit 7: History & Economics of Cyber – Big Ideas 5, 6, 8
Unit 8: Secure Software – Big Ideas 5, 7
Unit 9: Security and Vulnerabilities – Big Ideas 2, 3, 4, 5, 6, 7

Instructional Setting

School	Bollman Technical Education Center in Thornton, Colorado is the Career and Technical Education Center for the Adams 12 Five Star School District. Students come from all five of the Comprehensive High Schools in the district and one of the charter schools in the district. This cybersecurity course is an elective course open to (10th - 12th grade) students who have met the prerequisites necessary for the class. The average class size is 15 - 20 students.
Student Population	This cybersecurity course has the following demographics: ● 26% ELL ● 20% Gifted and Talented ● 6% on IEP / 504 ● 20% Free / Reduced Lunch ● 13% Charter School Students ● 87% District Comprehensive High School Students
Instructional Time	This is a yearlong course with 4 class periods a week at 55 minutes and 1 class period a week at 30 minutes.
Student Preparation	This course is open to 10th - 12th grade students who have taken either AP Computer Science A or AP Computer Science Principles or have received instructor approval.
Primary Planning Resources	Resources are listed in the materials section of each unit.

Overview of the Course

Course Goals

The goal of this course is for students to gain a basic understanding of cybersecurity through technical reading, videos, podcasts, class discussions, hand-on applications, simulations, and board games.

Students are assessed in multiple ways including written exams, quick writes, reflections, hands-on exercises, and simulations.

Cybersecurity Curriculum Guidelines Mapping

Unit Number	Big Idea	Enduring Understanding	Learning Objective	Essential Knowledge Statement
1: Law and Ethics	1 Ethics, 4 Data Security, 5 System Security, 8 Implications	1.1 EU: Social goals reflect the foundational values held by society; these core societal values are reflected in cybersecurity choices. 1.2 EU: Ethical reflection and judgement are required in considering the potential harms, benefits, and trade-offs involved in cybersecurity. 1.3 EU: Cybersecurity practices are highly complex and variable causing tensions between what the ethical duties are, to whom the ethical concern	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. 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. 1.2.1 LO: Students will discuss how cybersecurity can significantly impact the quality of people's lives both positively and negatively. 1.3.1 LO: Students will explore the tensions that exist between transparency, autonomy, resilience and security. 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. 1.3.3 LO: Students will discuss how even when a cybersecurity practice is legal, it may not be ethical. 4.1.1 LO: Students will analyze existing data security concerns and assess methods to overcome those concerns. 4.2.1 LO: Students will compare and contrast data protection legislation,	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. 1.1.1d EK: Different communities and societies have different foundational social goals and values that impact their behaviors concerning technology. 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. 1.2.1a EK: Examples in history demonstrate the harms and benefits of cybersecurity from multiple perspectives. 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. 1.2.1c EK: Cybersecurity requires resources, including time, money, and expertise that also affects technological affordances.

		should be considered, and whose interests should be invested in protecting. 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. 5.4 EU: Software and Hardware (or Systems) are everywhere which increasingly makes it	policies, and procedures that have been or are being introduced all over the world to protect personal data. 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 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. 8.3.3 LO: Students will describe how economics shape the decisions of consumers.	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. 1.3.2a EK: Ethical obligations are a set of "ought to" standards 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. 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. 1.3.3c EK: Using the anonymity of the internet for behavior that can harm others may not be illegal. 1.3.3d EK: Disclosure of software vulnerabilities to a party other than the software developer is legal and can be harmful. 4.1.1a EK: Data reveals 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.

		foundational in civilization. 8.1 EU: Cybersecurity shapes and is shaped by significant historical ideas and events. 8.2 EU: Cybersecurity is global, transcending traditional boundaries, and is always evolving. 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.		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: CFFA (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 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. 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). 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. 8.1.1c EK: Events in cyber warfare and cybercrime escalated the need for increased cybersecurity efforts. 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. 8.2.1c 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. 8.2.1f 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. 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.
2: CIA Triad	2 Establishing Trust, 4 Data Security, 8 Implications	2.1 EU: Cybersecurity relies on confidentiality, integrity, and availability (the CIA triad). 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	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. 4.1.1 LO: Students will analyze existing data security concerns and assess methods to overcome those concerns. 8.1.1 LO: Students will summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field	2.1.1a EK: Confidentiality is the protection of information from disclosure to unauthorized parties 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. 2.1.3a EK: 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: There is a tradeoff between 1) confidentiality and integrity and 2) availability. 4.1.1c EK: Data must be protected in processing, transmitting and storage. 4.1.1e EK: Data integrity means only authorized changes are made only by authorized people.

		access privilege to it. 8.1 EU: Cybersecurity shapes and is shaped by significant historical ideas and events.		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. 8.1.1e EK: The violation of system integrity can alter the behavior of critical infrastructure. 8.1.1f EK: A loss of availability has disrupted critical business functions.
3: Hardware & Software Basics	2 Establishing Trust, 5 System Security	2.3 EU: The more you restrict access, processes, resources, and users based on the policy, the more secure the system. 5.1 EU: Systems consist of a combination of hardware and software that together achieve some objective and security requires integration of both. 5.2 EU: Hardware security protects the machine and peripheral hardware from theft and from electronic intrusion and damage.	2.3.2 LO: Students will know that the principle of process isolation prevents tampering or interference from/by other processes. 5.1.1 LO: Students will identify how hardware and software work together in complex ways to achieve an overall objective. 5.2.1 LO: Students will convey that computer hardware refers to the physical parts of a computer and related devices.	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. 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. 5.2.1c 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. 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. 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. 5.2.1a EK: Internal hardware devices include motherboards, hard drives, and memory. 5.2.1b EK: External hardware devices include monitors, keyboards, mice, printers, scanners, routers, switches, servers, IoT devices industrial control systems, security cameras, etc.

4: Computer System Security (Image Hardening)	2 Establishing Trust, 4 Data Security, 5 System Security	2.1 EU: Cybersecurity relies on confidentiality, integrity, and availability (the CIA triad). 2.3 EU: The more you restrict access, processes, resources, and users based on the policy, the more secure the system. 2.4 EU: Identifying and questioning assumptions is a key part of making a system more secure. 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.	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. 2.4.1 LO: Given a scenario, students will identify the assumptions made in the design of the system and evaluate the trade-offs involved in defending a system while determining whether these assumptions hold in its execution. 4.2.3 LO: Students will evaluate and recommend technical controls that can be used to secure data. 4.3.1 LO: Students will define cryptography and explain how it is used in data security. 5.1.1 LO: Students will identify how hardware and software work together in complex ways to achieve an overall objective.	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. 2.1.2a EK: Integrity is the trustworthiness of data or resources. 2.1.2c EK: Data integrity is the information changing in authorized ways by authorized people, often called authentication. 2.1.3a EK: 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. 2.4.1a 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. 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. 4.3.1j EK: Hash functions can be used for checking whether a file was corrupted. 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.

		4.2 EU: Data Security uses non-technical and technical controls and techniques to protect data that is being processed, transmitted and stored. 4.3 EU: Cryptography techniques are necessary to keep data private and secure, and evolve with changes in technology. 5.1 EU: Systems consist of a combination of hardware and software that together achieve some objective and security requires integration of both.		
5: Cryptography	2 Establishing Trust, 4 Data 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 4.3.1 LO: Students will define cryptography and explain how it is used in data security.	2.1.1c EK: Cryptography is necessary to ensure confidentiality and integrity. 2.1.1d EK: Hiding is another aspect of confidentiality. 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.

	7 Risk, 8 Implications	4.3 EU: Cryptography techniques are necessary to keep data private and secure, and evolve with changes in technology. 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. 8.1 EU: Cybersecurity shapes and is shaped by significant historical ideas and events.	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. 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. 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.	4.3.1c EK: Cryptographic algorithms, also known as ciphers, 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. 4.3.1k 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 EK: 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. 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. 7.2.4h EK: Certificate authorities play a role in asserting the identities. 8.1.2c EK: Early government policies discouraged the use of encryption to build secure networks.
6: Networks, The Internet and IOT	1 Ethics, 3 Ubiquitous Connectivity, 5 System Security, 6 Adversarial Thinking, 7 Risk, 8 Implications	1.1 EU: Social goals reflect the foundational values held by society; these core societal values are reflected in cybersecurity choices. 1.2 EU: Ethical reflection and judgement are required in considering the potential harms, benefits, and trade-offs involved in cybersecurity.	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. 1.2.2 LO: Students will give examples of where/how tools are used in ways that were not intended by the system designer. 3.1.1 LO: Students will explain how devices use layers to communicate across the Internet and describe the purpose of the layers 3.1.2 LO: Students will explain how network standards and protocols allow different types of devices to communicate. 3.2.3 LO: Students will identify and distinguish between the purposes of network security devices and technologies.	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. 1.2.2a 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. 1.2.2b 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. 3.1.1a EK: Networks carry two types of information, those that allow for the controlling of the data and the data itself. 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, Wifi (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 EU: The Internet is a large, globally distributed network that is divided into layers, governed by protocols, and connects a wide variety of devices. 3.2 EU: The Internet provides a large attack surface, which offers efficiencies or economies of scale for adversaries. 5.4 EU: Software and Hardware (or Systems) are everywhere which increasingly makes it foundational in civilization. 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 EU: There are factors that	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. 5.4.2 LO: Students will predict how physical systems that rely on software may be vulnerable to future attacks. 6.1.1 LO: Students will explain how cybersystems are complex systems. 6.1.2 LO: Students will explain how complexity impacts the failure of cybersystems. 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. 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. 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.	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.) define their own protocols and are implemented at the application layer. 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: Protocols like the Domain Name System (DNS) provide a mechanism to map names like "www.example.com" into the IP addresses used for communication. Using words instead of memorizing numbers makes for faster and easier navigation of the internet. 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. 3.2.3a 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.

		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. 8.1 EU: Cybersecurity shapes and is shaped by significant historical ideas and events.		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. 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). 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. 5.4.2b 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.

				5.4.2c EK: Increased industry connectivity will cause increased attacks from adversaries such as cyber criminals, disgruntled employees, terrorists, organized crime, and nation states. 5.4.2d EK: Vulnerabilities may allow adversaries to interfere with connected devices. 5.4.2e EK: The consequences of unintentional faults or malicious attacks could have severe impact on human lives and the environment. 5.4.2f EK: By targeting trusted resources attackers can control devices and wholeheartedly manipulate users. 5.4.2g EK: By targeting trusted resources attackers can control devices and wholeheartedly manipulate users. 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. 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. 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. 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. 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. 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. 8.1.2a EK: The Internet provides global connectivity and is not structured around national boundaries. 8.1.2b EK: Security was not seen as a concern until much of the "infrastructure" for computer networks was in place. 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.
7: History & Economics of Cyber	5 System Security, 6 Adversarial Thinking, 8 Implications	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 makes it foundational in civilization. 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 EU: Cybersecurity shapes and is shaped by	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. 6.1.4 LO: Students will understand how social behaviors and human factors impact the cybersecurity of a system design. 8.1.1 LO: Students will summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field. 8.2.1 LO: Students will describe how political ideologies, economic structures, social organizations, and cultural perceptions impact cybersecurity. 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.	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. 5.2.3a 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. 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. 8.1.1a EK: Information campaigns were used and considered vital throughout history. 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. 8.1.1c EK: Events in cyber warfare and cybercrime escalated the need for increased cybersecurity efforts.

		significant historical ideas and events. 8.2 EU: Cybersecurity is global, transcending traditional boundaries, and is always evolving. 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.	8.3.3 LO: Students will describe how economics shape the decisions of consumers.	8.1.1d EK: The loss of confidentiality is a critical factor in warfare. 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. 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. 8.2.1d 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. 8.3.1a 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. 8.3.1d EK: When misaligned incentives arise, the party making the security–efficiency trade-off is not the one who loses out when attacks occur. 8.3.2a 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.

				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.
8: Secure Software	5 System Security, 7 Risk	2.3 EU: The more you restrict access, processes, resources, and users based on the policy, the more secure the system. 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. 7.1.4 LO: Students will be able to conduct standard security testing and 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.	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).

		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		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. 7.1.4b EK: Known vulnerabilities can be found in databases that collect, maintain, and disseminate information. 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. 7.2.3a 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.
9: Security and Vulnerabilities	2 Establishing Trust, 3 Ubiquitous Connectivity, 4 Data Security,	2.1 EU: Cybersecurity relies on confidentiality, integrity, and availability (the CIA triad). 2.2 EU: The simpler you can make the design or implementation of a system, the	2.1.3 LO: Students will evaluate methods of protecting information and information systems from disruption and destruction. 2.2.1 LO: Students will explore the principle of simplicity, which is about how users can easily translate their general protection goals to appropriate system security configurations. 2.2.2 LO: Students will use the principle of abstraction to represent complicated concepts more simply and to allow	2.1.3d EK: Assuring availability includes prevention, detection, and response mechanisms. 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. 2.2.3a 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.

	5 System Security, 6 Adversarial Thinking, 7 Risk	better you can check whether or not it can be exploited. 2.3 EU: The more you restrict access, processes, resources, and users based on the policy, the more secure the system. 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. 3.2 EU: The Internet provides a large attack surface, which offers efficiencies or economies of scale for adversaries. 4.2 EU: Data Security uses non-technical and technical controls and techniques to protect data that is being	solutions to be transferred to other contexts. 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 explore the principle of domain separation, which allows for the enforcement of rules governing the entry and use of domains by entities outside the domain. 2.3.3 LO: Students will know that the principle of resource encapsulation allows access or manipulation of the resource only in intended ways. 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 explore 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 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 principle of modularity is a design technique that separates the functionality of a program into	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. 2.3.3a EK: Examples of resources are the memory, disk drive, network bandwidth, battery power, and a monitor. 2.3.3b EK: In programming, resource encapsulation is one of the main principles of object-oriented design. 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. 2.3.7a EK: A component cannot be modular without a well-designed interface and an important aspect of modularization is not just how you interact with it but that it has minimum side effects. 2.3.7b EK: A system's components may be separated and recombined. 2.3.8a EK: When something does not work, the system must return to a secure state. 2.3.8b EK: When a system fails it must fail into a safe state.

		processed, transmitted and stored. 5.2 EU: Hardware security protects the machine and peripheral hardware from theft and from electronic intrusion and damage. 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. 6.1 EU: Adversity comes from anyone or anything where the end result differs from that intended by the system designer and user. 6.2 EU: Adversarial thinking is the process of	independent components. Each component is self-sufficient and capable of executing a unique part of the desired functionality through well-designed interfaces. 2.3.8 LO: Students will explore the principle of fail-safe defaults, which restricts how privileges are initialized when a subject or object is created. 3.1.2 LO: Students will explain how network standards and protocols allow different types of devices to communicate. 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. 4.2.2 LO: Students will identify physical controls that are used to secure data. 4.2.3 LO: Students will evaluate and recommend technical controls that can be used to secure data. 5.2.2 LO: Students will know some common hardware-related vulnerabilities. 5.2.4 LO: Students will identify hardware security addresses issues related to an adversary physically gaining access to a device. 5.3.3 LO: Students will describe the process of validating that software remains secure through its lifecycle.	2.3.8c EK: Turning off permission causes a security problem 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 and is largely discredited as a security solution. 3.1.2f EK: Cryptographic algorithms are either publicly known or proprietary and have the same security through obscurity tradeoffs 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 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, two primary attacks an adversary might take is to spoof (forge) a source address and the other is to cause a Denial of Service (DoS) attack. 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. 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.

		reasoning about how opposing forces could prevent a system from meeting both its functional and security goals. 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. 7.2 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.	6.1.3 LO: Students will understand how different system components impact the cybersecurity of a system design. 6.2.1 LO: Students will know how natural events and unintentional errors can cause a system to fail. 6.2.2 LO: Students will know how intentional attacks can adapt to defenses and cause a system to fail. 6.2.3 LO: Students will analyze how the cybersecurity attack lifecycle/kill chain is essential to adversarial thinking. 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. 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. 7.2.2 LO: Students will be able to describe how the presence of an adversary necessitates that cybersecurity risk is emergent and complex. 7.2.3 LO: Students will be able to explain how the logical malleability of software and hardware can allow an adversary to	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. 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. 4.2.3j EK: Failure to protect data can be due to faulty authentication, faculty authorization, and/or faulty access control. 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. 5.2.4a EK: The hardware design can require the device to disable itself if physically tampered with. 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. 5.3.3a EK: A security analysis is a process that is used to verify a program meets a specified list of security requirements.

			change a system to meet the adversary's goals rather than the systems original objective. 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.	5.3.3b EK: Security vulnerability reports (CWE and CVE) are publicly available for software systems and should be monitored, or subscribe to their alerts. 5.3.3c EK: Zero-day attacks are vulnerabilities that were not knowledge until they were encountered. 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. 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. 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. 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.

				6.2.3a EK: The term “kill chain” refers to the structure—or seven stages—of a cyberattack. 6.2.3b EK: 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 EK: 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 EK: 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 EK: Exploitation is the fourth phase where the code is triggered exploiting vulnerable applications or systems. 6.2.3f EK: 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 EK: 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 EK: 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. 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. 7.1.4a EK: Vulnerability assessment identifies known vulnerabilities on the system. 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 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. 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. 7.2.3d EK: Hardware itself may act in unintended ways and an adversary is seeking to find and exploit these unintended behaviors. 7.2.4i EK: Cryptography does not solve operational challenges and cryptography alone is not a solution in a decentralized network.

Pacing

Unit	Hours of Instruction	Unit Summary
1. Law & Ethics	13 - 16	Students learn how core societal values shape security considerations of designers and users and why privacy is essential for individuals, groups and government. Students also learn how cybersecurity ideas and events have impacted society.
2. CIA Triad	6 - 7	Students learn how confidentiality, integrity, and availability are all interconnected.
3. Hardware & Software Basics	3 - 4	Students learn how hardware and software work together to achieve an objective.
4. Computer Systems Security (Image Hardening)	7	Students learn what policies and procedures are put in place to keep data safe through a hand-on lab using a Windows image.
5. Cryptography	16 - 17	Students identify and demonstrate ways data can be encrypted.
6. Networks, The Internet & IOT	24 - 27	Students learn how the Internet organized and what role standards and protocols play in keeping networks secure.

7. History & Economics of Cyber	6 - 8	Students learn how risk management and economic tradeoffs impact cybersecurity decisions, how historical ideas and events have impacted society, and how the expansion of the threat environment has been addressed in society.
8. Secure Software	10 - 13	Students learn why software has security vulnerabilities, what the vulnerabilities are and the consequences of less secure software.
9. Security and Vulnerabilities	23 - 30	Students learn how cybersecurity risk is modeled; the difference between a risk, vulnerability, and a threat; how simplicity and restriction are overarching ideas for cybersecurity principles; and what security flaws/ vulnerabilities are in hardware and software.

Detailed Unit Descriptions

UNIT 1: LAW AND ETHICS

Estimated Time in Hours: 13-16

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
1 Ethics 4 Data Security 5 System Security 8 Implications	1.1, 1.2, 1.3, 4.1, 4.2, 5.4, 8.1, 8.2, 8.3	- Create a Country - Silent Debate (Technology & Law) - Harms & Benefits Reflection on Intellectual Property - Privacy Laws Presentation - Privacy vs. Security Debate - Law and Ethics Game

Guiding Questions:

- How do values shape the security considerations of designers?
- How do values shape the security considerations of users?
- How do core societal values shape the security considerations in what is allowed or encouraged to be created?
- Why is privacy essential for individuals, groups, and governments?
- How have historical cybersecurity ideas and events impacted society?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
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. EK: 1.1.1a	• KWL Chart (find example KWL chart at https://www.timvandevall.com/templates/kwl-chart-template/) • Jackson, Tom. *Activities that Teach*. Red Rock Publishing, 1993.	**The Connection Between Values, Ethics & Society: (2-day lesson)** Students identify values in their lives and the lives of their classmates. • This lesson begins with a KWL pre-assessment on values. In order to help students understand their values and the values of their classmates, students complete the Auction Activity from "Activities That Teach". The auction has

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. EK: 1.1.2e 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. EK: 1.3.2a,b	• "Ethics". *BrainPOP.com*, https://www.brainpop.com/health/personalhealth/ethics/ • Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Poster Paper • Markers • Notebook	items that will help students identify what they value. Once the auction is complete, students discuss what they value based on purchases that were made in the class auction. Students then return to the KWL and update it. Then, students gain an understanding of how values relate to ethics. • Students are introduced to ethics through a video, then read section 19.4 - Ethical Issues in the textbook (p.596-601). Students respond to review question 19.13 in their notebook. Students then discuss how ethics relate to values. Finally, students understand how values and ethics relate to the creation of societies. • Students work in groups to create a country, naming the country, creating the money, flag, government structure & laws. Once students create their country and share-out, they discuss how they created their society and how the society was a group of individuals characterized by common interests/values. • The lesson is wrapped up with students adding vocabulary to their notebook. In the notebook students define their vocabulary word, write the impact - why it is important, and add a picture to represent the word.
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.	• Notebook • "The Harm Principle – Learn Liberty." *YouTube*, uploaded by Learn Liberty, 21 June 2011,	**Technology and Law: (1-2-day lesson)** In this lesson students learn the difference between a crime and an unethical decision and can evaluate the arguments of the nature of crime and be able to develop their own understanding of the uses of technology that should be criminal.

EK: 1.1.1b,d 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. EK: 1.1.2a 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. EK: 1.3.2a,b	https://www.youtube.com/watch?v=Z03OXBbLr40&feature=youtu.be • "Hackers Remotely Kill a Jeep on the Highway–With Me in It." Wired Magazine, *Wired.com*, 21 July 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ • Silent Debate Materials, e.g., a worksheet or a large piece of paper, colored pens/pencils (for instructions on Silent Debates, visit https://teach.nflc.umd.edu/startalk/classroom-activity/silent-debate-38) • Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015.	• Students begin by watching the harm principle video and respond to the following questions in their notebook: "Why does Mill think harm is appropriate for criminal punishment? What sorts of harms do we deal with today that did not occur in Mill's time? Are those harms appropriate for criminal punishment? What about hacking?" The class discusses the responses students wrote in their notebooks. Students then read the article and watch the video on the Jeep Hacking. Students complete a silent debate about the Jeep Hacking incident. Students then read section 19.1 in the textbook - Cybercrime and Computer Crime (p. 579-583). After reading the text, students discuss their arguments from the silent debate and compare their thoughts with what they learn about cybercrime and computer crime.
1.1.1 LO: Students will analyze online and offline behaviors in societies, i.e., themselves, peers,	• Notebook • Intellectual Property Poll • Textbook:	**Intellectual Property: (1-2-day lesson)** In this lesson students learn about intellectual property and how society impacts laws around it.

families, communities, and countries, and deduce the values that govern these behaviors. EK: 1.1.1a,d 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. EK: 1.1.2b,d 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. EK: 4.2.1g	Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Cornell Notes (for an explanation of the Cornell note-taking system, visit http://lsc.cornell.edu/study-skills/cornell-note-taking-system/) • "SOPA and 3 Ways to think about Intellectual Property." *YouTube*, uploaded by Learn Liberty, 18 Mar 2013, https://www.youtube.com/watch?v=fiFDLuhIq7M&feature=youtu.be • "Online Piracy… It's Different." *YouTube*, uploaded by runofkings, https://www.youtube.com/watch?v=7JSrrxb85FY&feature=youtu.be • "Piracy it's a crime." *YouTube*, uploaded by haxorcat, 4 Dec 2007,	• This lesson begins with students taking a poll about intellectual property. Class discussion about the results of the poll the students took. Students then read section 19.2 - Intellectual Property in the textbook (p. 583-589) and take Cornell notes. Students then watch the video on intellectual property. Students then discuss the values that intellectual property protection is intended to serve and how acceptable use policies play a role in this. Students watch the two videos on piracy and read *Automated Crimes - Automated Justice* p.195-199 in Blown to Bits. Students then answer questions in their notebook about the benefits and costs of intellectual property.

	https://www.youtube.com/watch?v=HmZm8vNHBSU&feature=youtu.be • Abelson, Ledeen, and Lewis. *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*. Addison-Wesley Professional, 2008.	
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. EK: 1.1.1b,d 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. EK: 1.1.2a,c,d 1.2.1 LO: Students will discuss how cybersecurity can significantly impact the quality	• Podcast (start at 4 min 45 sec): Schneier, Bruce and Henage, Dan. "Crypto-Gram February 15, 2020." *The Crypto-Gram Security Podcast*, Libsyn, 15 Feb 2020, https://hwcdn.libsyn.com/p/4/f/f/4ff722d465bd469f/crypto-gram-2020-02.mp3?c_id=66980507&cs_id=66980507&destination_id=19374&expiration=1595259639&hwt=c2fa9cb974afdf7902e22a29f4a7b4df • Textbook:	**Privacy: (7 -8-day lesson)** In this lesson students learn about how society impacts law around privacy and how digital technology plays a role in privacy. • The lesson begins with students listening to the podcast linked left (listen to the section on Modern Mass Surveillance, beginning at 4 min 45 sec). The class then discusses what they heard in the podcast about technology, law and society. Students then read section 19.3 - Privacy (p.589-595) in the textbook & The European Data Protection Rules, where they learn about privacy and laws around privacy. Students are given a list of privacy laws and broken up into groups. Each group is assigned a law to research and present to the class. Students then learn about their electronic record and the impact technology has on their privacy. They begin by watching the internet privacy prank, followed by the online safety commercial. Students then read "Social Media Raises Privacy and Ethics Issues" from USA Today and articles supplied by the teacher (e.g., on topics such

of people's lives both positively and negatively. EK: 1.2.1a,b,c 1.3.1 LO: Students will explore the tensions that exist between transparency, autonomy, resilience and security. EK: 1.3.1a,b,c,d 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. EK: 1.3.2a,b 1.3.3 LO: Students will discuss how even when a cybersecurity practice is legal, it may not be ethical. EK: 1.3.3b,c 4.1.1 LO: Students will analyze existing data security concerns and assess methods to overcome those concerns. EK: 4.1.1a,b,c,d,e,f,g	Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • "EU data protection rules." European Commission, *ec.europa.eu*, https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en • "Internet Privacy Prank." *YouTube*, uploaded by BuzzFeedVideo, 3 Apr 2014, https://www.youtube.com/watch?v=YLWmjpPoJHk&feature=youtu.be • "Bulletin Board - Online Safety Commercial." *YouTube*, uploaded by OhioCommissionDRCM, https://www.youtube.com/watch?v=nOUu1fldBbI&feature=youtu.be • Jayson, Sharon. "Social media raises privacy and ethics issues." USA Today,	as how colleges use Facebook to research potential students or how employers use social media to research potential employees). The class has a discussion on how what they post online is permanent and can have an impact on their future. Students then research themselves to see what they can find in their electronic record. They report out using a Voki. Students then investigate the World's Biggest Data Breaches Website and identify data breaches that may have caused them to lose some of their private information. Students reflect in their notebook about the possible data they have lost and how it could impact their future. Students then read the Tanya Rider story in Blown to Bits (p. 1-2). Students discuss the harms and benefits of privacy when it came to the Tanya Rider story using a Community Circle. Students read the Declaration of Independence and the Bill of Rights. Students use the notes that they have taken on their learning throughout this lesson and use them along with the information that they attain from reading the Declaration of Independence and the Bill of Rights. Students write a persuasive argument citing evidence to answer the following question: "When security and liberty come into conflict, which one should take precedence?" The lesson is wrapped up with a debate about security vs. privacy, using the arguments that the students wrote.

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. EK: 4.2.1a,b,c,d,e,f 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. EK: 5.4.1a 8.2.1 LO: Students will describe how political ideologies, economic structures, social organizations, and cultural perceptions impact cybersecurity. EK: 8.2.1c 8.2.2 LO: Students will analyze how privacy concerns vary greatly in regards to societies, age, and socio-economic status. EK: 8.2.2b	*USAToday.com*, 8 Mar 2014, https://www.usatoday.com/story/news/nation/2014/03/08/data-online-behavior-research/5781447/ • "World's Biggest Data Breaches & Hacks." *InformationisBeautiful.net*, https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ • Abelson, Ledeen, and Lewis. *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*. Addison-Wesley Professional, 2008. • "America's Founding Documents | Declaration of Independence: A Transcription." National Archives, *Archives.gov*, https://www.archives.gov/founding-docs/declaration-transcript	

	• "America's Founding Documents | The Bill of Rights: A Transcription." National Archives, *Archives.gov*, https://www.archives.gov/founding-docs/bill-of-rights-transcript	
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. EK: 1.1.2c 1.2.1 LO: Students will discuss how cybersecurity can significantly impact the quality of people's lives both positively and negatively. EK: 1.2.1a,b,c 1.3.3 LO: Students will discuss how even when a cybersecurity practice is legal, it may not be ethical. EK: 1.3.3a,d 8.1.1 LO: Students will summarize and interpret the	• "How Dangerous are Hackers: Cyber Warfare Documentary 2019." *YouTube*, uploaded by Breed Skool, 10 Mar 2019, https://www.youtube.com/watch?v=NY3SpIQHD2I&feature=youtu.be • Note catcher (for an example note catcher, see http://www.cte.iup.edu/preinduction/HO_Video%20Note%20Taking%20Worksheet.pdf)	**Cybersecurity - Impacts, Laws and Ethics: (3-day lesson)** In this lesson students learn about the impacts of cybersecurity and how even when a cybersecurity practice is legal, it may not be ethical. • Students watch How Dangerous are Hackers and take notes on the note catcher. There is then a class discussion about the law, ethics and impacts addressed in the video. **Assessment:** *Students create a board game to review everything they learned about the impacts of law and ethics in cybersecurity in a fun and interesting way.* *Board Game Requirements:* • *Using a file folder, colored pencils, crayons, or markers, create a board game. Put the name of your game on the tab of the folder and decorate the inside so that it is a game board.* • *Make your game board neat, colorful, interesting and creative.* • *Create at least 25 questions and answers for your game that relate to the material covered in the Law & Ethics Unit. Be sure to include key vocabulary from the unit.*

impact of cybersecurity ideas and events on the evolution of the field. EK: 8.1.1b,c,g 8.2.1 LO: Students will describe how political ideologies, economic structures, social organizations, and cultural perceptions impact cybersecurity. EK: 8.2.1f,g 8.2.2 LO: Students will analyze how privacy concerns vary greatly in regards to societies, age, and socio-economic status. EK: 8.2.2a,c 8.3.3 LO: Students will describe how economics shape the decisions of consumers. EK: 8.3.3b,c		*The questions must somehow be incorporated into the playing of the game.* • *Relate the format and purpose of your game to one of the themes you learned about in the Law & Ethics Unit.* • *Write directions for your game that would make it perfectly clear how to play the game. The directions need to be typed and glued on the back cover of the file folder.* • *Make sure you have different difficulty levels in your game in order to help all students review and learn the content from the unit. Be sure to think about 2nd language learners in the class and how you can help them understand the content (examples: translate questions to another language, include images, etc.).*

UNIT 2: CIA TRIAD

Estimated Time in Hours: 6-7

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 4 Data Security 8 Implications	2.1, 4.1, 8.1	- Round Table Discussions - Key Vocabulary / Concepts Poster - CIA Triad Problems

Guiding Questions:

- How are confidentiality, integrity, and availability interconnected?
- What is essential for establishing trust in cybersecurity?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
2.1.1 LO: Students will evaluate methods of keeping information secret from those whom the information should be kept secret EK: 2.1.1a,e 2.1.2 LO: Students will demonstrate that integrity involves trust and credibility. EK: 2.1.2a,b,c,d 2.1.3 LO: Students will evaluate methods of protecting information and information systems from disruption and destruction. EK: 2.1.3a,b	• "Cybersecurity: Crash Course Computer Science #31." *YouTube*, uploaded by CrashCourse, 11 Oct 2017, https://www.youtube.com/watch?v=bPVaOlJ6ln0&feature=youtu.be • Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Window Notes Sheet (access a blank Window Notes template at https://toolsforclassroominstructionthatworks.com/	**Introduction to CIA and Key Vocabulary: (5-day lesson)** Students will learn what cybersecurity is and the key concepts to the CIA Triad. • In this lesson the basics of cybersecurity and the CIA Triad is introduced. Students begin with an introduction video to Cybersecurity. They learn the basics of cybersecurity. Students then read about the concepts that make up the CIA Triad in the textbook: "*Computer Security Principles and Practice - Third Edition"* by William Stallings & Laurie Brown. They read section 1.1, 1.2, and 1.6 and take Window notes on each section. They then share their notes with a group of 3-4 students and discuss what they have learned. They add to their notes based on the discussion with their peers. After the discussions students research and analyze methods for keeping information secret. They write an argument for the method they think is best. Students then have a round table discussion regarding the best method of keeping information secret using the arguments they have written. Students

4.1.1 LO: Students will analyze existing data security concerns and assess methods to overcome those concerns. EK: 4.1.1c,e,f,g	wp-content/uploads/2018/01/Window-Notes.pdf) • Poster Paper • Markers	research and analyze methods of protecting information and information systems from disruption and destruction. They write an argument for the method they think is best. Students then have a round table discussion regarding the best method of protecting information using the arguments they have written. Students then create key concepts/ vocabulary image posters and share out their posters.
2.1.3 LO: Students will evaluate methods of protecting information and information systems from disruption and destruction. EK: 2.1.3c 8.1.1 LO: Students will summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field. EK: 8.1.1e,f	• Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Notebook • Think in Threes Note Catcher	**Understanding Implications of CIA Triad: (1- 2-day lesson)** Students will apply their knowledge of the CIA Triad to problems to demonstrate their understanding of the implications of CIA. • In this lesson students begin with a warm-up defining *Computer Security* in their notebooks. Students will then complete problems 1.1, 1.3, and 1.4 parts a-d from the textbook. Once the students complete the problems they discuss their answers with a partner. The lesson is wrapped up with a class discussion about the tradeoffs between confidentiality, integrity, and availability. Along with the impacts to business and critical infrastructure. **Assessment:** *Using a Think in Three note catcher, students define the three parts of the CIA triad and write a paragraph explaining the CIA Triad in the box at the bottom of the note catcher. Students then complete Problem 1.4-part e from the textbook.*

UNIT 3: HARDWARE AND SOFTWARE BASICS

Estimated Time in Hours: 3-4

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 5 System Security	2.3, 5.1, 5.2	- Hardware T-Chart - Three Column Notes on a Process - Project: Hardware & Software Working Together

Guiding Questions:

- How do hardware and software work together to achieve an objective?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
5.1.1 LO: Students will identify how hardware and software work together in complex ways to achieve an overall objective. EK:5.1.1a,b 5.2.1 LO: Students will convey that computer hardware refers to the physical parts of a computer and related devices. EK: 5.2.1a,b,c,d	• Window Notes Sheet (access a blank Window Notes template at https://toolsforclassroominstructionthatworks.com/wp-content/uploads/2018/01/Window-Notes.pdf) • Notebook • CyberPatriot Training Materials | Unit 5: Computer Basics and Virtualization. *USCyberPatriot.org* (use Unit 5 Section 1 only; must register as a Coach, Mentor, or Team Assistant to see the most recent training materials)	**Understanding hardware and software: (1-day lesson)** Students gain an understanding of the difference between hardware and software and are able to define hardware and software. • In this lesson students use the window notes they took in Unit 2. They begin by defining hardware and software in their notebooks. Students then learn about how computers work. Begin with the anatomy of a computer, followed by the BIOS, and software. The class discusses hardware (be sure to address 5.2.1c,d in the discussion) and creates a T-chart identifying internal and external hardware. The class then discusses software and takes notes on the discussion.

	• Poster Paper • Markers	
2.3.2 LO: Students will know that the principle of process isolation prevents tampering or interference from/by other processes. EK:2.3.2a,b	• KWL Chart (find example KWL chart at https://www.timvandevall.com/templates/kwl-chart-template/) • Three Column Notes (for an example of a 3-column note chart, visit https://www.teacherspayteachers.com/Product/Three-Column-Chart-Graphic-Organizer-Critical-Thinking-Skills-220940) • "The Central Processing Unit (CPU): Crash Course Computer Science #7." *YouTube*, uploaded by CrashCourse, 5 Apr 2017, https://www.youtube.com/watch?v=FZGugFqdr60&feature=youtu.be • "Instructions & Programs: Crash Course Computer Science #8." *YouTube*, uploaded by CrashCourse, 12 Apr 2017,	**Understanding the CPU & Instructions: (1-day lesson)** Students will gain an understanding of the CPU and how processes have an address space which only it can access. • In this lesson students begin by accessing prior knowledge. As a class, create a KWL chart about what students know about the CPU and processes. Students then use the three column notes to take a column of notes on each of the three videos that they watch about how the CPU runs and how instructions are stored in a region of memory. After students watch the first video, students share what they learned that is on their notes in column one with a partner. They updated their notes with anything they missed that their partner shared. The process is repeated with the 2nd and 3rd videos. The class is wrapped up with a class discussion about how a process is a program running on a computer, how each process has a region of memory which only it can access and how the CPU runs that process. The KWL chart is completed with what they learned and questions the students still have.

	https://www.youtube.com/watch?v=zltgXvg6r3k&feature=youtu.be • "Advanced CPU Designs: Crash Course Computer Science #9." *YouTube*, uploaded by CrashCourse, 26 Apr 2017, https://www.youtube.com/watch?v=rtAlC5J1U40&feature=youtu.be	
2.3.2 LO: Students will know that the principle of process isolation prevents tampering or interference from/by other processes. EK:2.3.2c 5.1.1 LO: Students will identify how hardware and software work together in complex ways to achieve an overall objective. EK:5.1.1a,b,c,e,f,g,h,i,j,k,l 5.2.1 LO: Students will convey that computer hardware refers to the physical parts of a computer and related devices. EK: 5.2.1a,b	• "How Computers Work: Hardware and Software." *YouTube*, uploaded by Code.org, 30 Jan 2018, https://www.youtube.com/watch?v=xnyFYiK2rSY&feature=youtu.be • Window Notes Sheet (access a blank Window Notes template at https://toolsforclassroominstructionthatworks.com/wp-content/uploads/2018/01/Window-Notes.pdf)	**Understanding How Computers Work: (1-2-day lesson)** Students learn about operating systems and how hardware and software work together. • In this lesson students start by watching the video on How Computers Work: Hardware and Software. While watching the video students take window notes. After the video, discuss as a class how processes have to use defined communications mediated by the operating system to communicate with other processes and how hardware and software work together to achieve an overall objective. Then, students are introduced to the project to reinforce their learning. **Assessment:** *Using everything the students learned in the Understanding hardware and software lesson and the video on how Computers Work: Hardware and Software students demonstrate their knowledge about hardware and software by creating a project to reinforce their peers' knowledge about hardware, software and how hardware and software work*

		together. The project could be a visual (sketch, model, etc.), a board game, a comic, etc. Students then present their project.

UNIT 4: COMPUTER SYSTEMS SECURITY

Estimated Time in Hours: 7

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 4 Data Security 5 System Security	2.1, 2.4, 4.1, 4.2, 4.3, 5.1	- Malware Poster - Hands-on Lab: Hardening a Windows Image

Guiding Questions:

- What policies and procedures are in place to keep data safe?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
2.1.1 LO: Students will evaluate methods of keeping information secret from those whom the information should be kept secret EK:2.1.1a,b 2.1.2 LO: Students will demonstrate that integrity involves trust and credibility. EK:2.1.2a,c 2.1.3 LO: Students will evaluate methods of protecting information and information systems from disruption and destruction EK:2.1.3a,b	• Notebook • Cornell Notes (for an explanation of the Cornell note-taking system, visit http://lsc.cornell.edu/study-skills/cornell-note-taking-system/) • CyberPatriot Training Materials | Unit 4: Principles of Cybersecurity. *USCyberPatriot.org* (must register as a Coach, Mentor, or Team Assistant to see the most recent training materials) • CyberPatriot Training Materials | Unit 5:	**Principles of Cybersecurity and Virtual Machines: (2-day lesson)** Students review the principles of the CIA Triad, learn about malware and about the use of a checksum - a hash function used to check if a file is corrupt. • This lesson begins with a lecture on the Principles of Cybersecurity and Virtual Machines. During the lecture, students complete Cornell Notes and update their notebooks with key vocabulary from the lecture. Students then create a poster about Malware in groups of 3-4 and present the posters to the class.

4.3.1 LO: Students will define cryptography and explain how it is used in data security. EK: 4.3.1j 5.1.1 LO: Students will identify how hardware and software work together in complex ways to achieve an overall objective. EK:5.1.1d	Computer Basics and Virtualization. *USCyberPatriot.org* (use Unit 5 Section 2 only) • CyberPatriot Training Materials | Unit 7: Microsoft Windows Security Tools. *USCyberPatriot.org* • CyberPatriot Training Materials | Unit 8: Microsoft Windows Security Configurations. *USCyberPatriot.org* • Poster Paper • Markers	
2.4.1 LO: Given a scenario, students will identify the assumptions made in the design of the system and evaluate the trade-offs involved in defending a system while determining whether these assumptions hold in its execution. EK: 2.4.1a,b,c,d,e 4.2.3 LO: Students will evaluate and recommend technical controls that can be used to secure data.	• Windows Image with vulnerabilities / issues • Checksum • VMWare	**Assessment: (5-day lesson)** *Students begin by running a checksum on the Windows Image you provide them to verify the integrity of the file. Students then load the Windows image in the VMWare and use the knowledge that they have gained over the last two days to harden the image by removing vulnerabilities and securing file permissions and access to the proper users.*

EK: 4.2.3f,g,h,i		

UNIT 5: CRYPTOGRAPHY

Estimated Time in Hours: 16-17

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 4 Data Security 7 Risk 8 Implications	2.1, 4.3, 7.2, 8.1	- Scytale & Caesar Cipher - Caesar Cipher Program - Anagrams - Symmetric Ciphers - Steganography - Public Key Encryption & Digital Signatures - History & Politics of Public Key Encryption - Breakout Box

Guiding Questions:

- What are the ways in which data can be encrypted?
- What actions can be taken to validate that data has been unaltered by an unauthorized source?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
2.1.1 LO: Students will evaluate methods of keeping information secret from those whom the information should be kept secret EK: 2.1.1c,d 4.3.1 LO: Students will define cryptography and explain how it is used in data security. EK: 4.3.1a,b,c,d,e,f,g,h,i 4.3.2 LO: Students will practice symmetric cryptosystems to	• KWL Chart (find example KWL chart at https://www.timvandevall.com/templates/kwl-chart-template/) • "Cryptography: Crash Course Computer Science #33." *YouTube*, uploaded by CrashCourse, 25 Oct 2017, https://www.youtube.com/watch?v=jhXCTbFnK8o&feature=youtu.be • Cornell Notes	**Introduction to Cryptology: (1-day lesson)** This lesson introduces students to cryptography and the history of cryptography. • Students begin with a pre-assessment using a KWL chart to identify what they know about cryptography. Students then watch the Cryptography Video. Students take Cornell notes on the video. Once the video is over, students return to the KWL chart and add to it based on what they have learned and what questions they still have. The class discusses the purpose of encryption, and how it is necessary to ensure confidentiality and integrity. Students then gain hands-on experience with two types of encryption. They begin by creating a scytale. Students select a pipe and wrap the crepe paper around it. Using a

send a message and explain how they work. EK: 4.3.2a,b,d,e 4.3.3 LO: Students will employ public key (asymmetric) encryption and explain how it works. EK: 4.3.3a,b,c,d	(for an explanation of the Cornell note-taking system, visit http://lsc.cornell.edu/study-skills/cornell-note-taking-system/) • PVC Pipe (with varying diameters) • Crepe Paper, Ribbon, or Washi Tape • Markers • Caesar Cipher Wheel • Paper	marker, they then write a message on the crepe paper. Next, they unwrap the message and pass their crepe paper message to someone else in the class to solve. The person solving the message must have a pipe that is the same length and diameter. After this activity, students discuss the strengths and weaknesses of this form of encryption. Students then create a wheel for the Caesar Cipher. Students encrypt a message for another student in the classroom using the Caesar Cipher. The message is then passed to the other student to decrypt. After this activity students discuss the strengths and weaknesses of this form of encryption.
4.3.1 LO: Students will define cryptography and explain how it is used in data security. EK: 4.3.1d,e,f,g,h	• Python	**Caesar Cipher Program: (2-3-day lesson)** In this lesson students build a program to encrypt and decrypt information using a Caesar Cipher. • Using Python students write a program that will ask the end user if they want to encrypt or decrypt a message. If the end user wants to encrypt a message the program asks for the message to encrypt and the key. The program then encrypts the message and outputs it to the end user. If the user selects to decrypt the message, the program asks the user to enter the encrypted message. It then outputs the value of each shift and the possible decryption for each shift.
4.3.2 LO: Students will practice symmetric cryptosystems to send a message and explain how they work. EK: 4.3.2c	• "Anagram in The da Vinci Code." *YouTube*, uploaded by Idan Cohen, 19 Oct 2013,	**Anagrams: (1-day lesson)** In this lesson students learn what anagrams are and how they are a way to attack a transposition cipher. • This lesson begins with students watching the "Anagram in The da Vinci Code" video, followed by the clip from

	https://www.youtube.com/watch?v=OZj8bxV7x9I&feature=youtu.be • "The Da Vinci Code (3/8) Movie CLIP – So Dark the Con of Man (2006) HD." *YouTube*, uploaded by Movieclips, 25 Oct 2012, https://www.youtube.com/watch?v=F_HKGZRUroE&feature=youtu.be • "Anagram Solver." Word Tips, *Word.Tips*, https://word.tips/anagram-solver/ • Paper • Pen or Pencil	"The Da Vinci Code" movie. Students discuss what they saw in the two videos. Students go to the word tips webpage and read about anagrams. Students then create an anagram for another student in the classroom. The other student will solve the anagram. The class is wrapped up with a class discussion about anagrams.
4.3.2 LO: Students will practice symmetric cryptosystems to send a message and explain how they work. EK: 4.3.2a,b,d,e	• Notebook • "Rail-Fence Cipher." Practical Cryptography, *PracticalCryptography.com*, http://practicalcryptography.com/ciphers/classical-era/rail-fence/ • "Baconian Cipher." Practical Cryptography, *PracticalCryptography.com*,	**Symmetric Cryptosystems: (7-day lesson)** In this lesson students practice using different symmetric cryptosystems. • Day 1 - In this lesson students will learn about the Rail-Fence Cipher. Students receive an assignment that is encrypted using a Caesar Cipher. They have to solve the Caesar Cipher in order to find out what they need to do in the assignments. The assignment asks the students to read about the rail-fence cipher at the practical cryptography website. Students add an explanation about how the rail-fence cipher into their notebook. Students are asked to encrypt a message telling their

	http://practicalcryptography.com/ciphers/classical-era/baconian/ • "Polybius Square Cipher." Practical Cryptography, *PracticalCryptography.com*, http://practicalcryptography.com/ciphers/classical-era/polybius-square/ • "Vigenère and Gronsfeld Cipher." Practical Cryptography, *PracticalCryptography.com*, http://practicalcryptography.com/ciphers/classical-era/vigenere-gronsfeld-and-autokey/ • "Four-Square Cipher." Practical Cryptography, *PracticalCryptography.com*, http://practicalcryptography.com/ciphers/classical-era/four-square/	favorite class in school using the rail-fence cipher and send it to another student to decode. The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the rail-fence method. • Day 2 - In this lesson students will learn about the Baconian Cipher. Students will receive an assignment that is encrypted using the Rail-Fence Cipher. They have to solve the Rail-Fence Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about the Baconian Cipher. Students add an explanation about how the Baconian cipher into their notebook. It also assigns students into teams to play Mission Code X and assigns the students the number of missions they are required to complete. Students are asked to encrypt a message using the Baconian cipher that they must send to a student in another game team that tells how successful they were in completing the missions in Mission Code X. A student from another team decodes the message. The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the Baconian method. • Day 3 - In this lesson students will learn about the Polybius Square Cipher. Students will receive an assignment that is encrypted using the Baconian Cipher. They have to solve the Baconian Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about the Polybius Square Cipher. Students add an explanation about how the Polybius Square cipher into their notebook. Students

	• "Playfair Cipher." Practical Cryptography, *PracticalCryptography.com*, http://practicalcryptography.com/ciphers/classical-era/playfair/ • Neijts, Semilof, Clark, and Rouse. "steganography." TechTarget|SearchSecurity, *SearchSecurity.com*, https://searchsecurity.techtarget.com/definition/steganography#:~:text=Steganography%20is%20the%20technique%20of,for%20hiding%20or%20protecting%20data. • Online Steganography tool: "Steganography (encode text into image)." Many Tools, *ManyTools.org*, https://manytools.org/hacker-tools/steganography-encode-text-into-image/ • Paper	are asked to encrypt a message about their favorite unit so far in Cybersecurity using the Polybius Square cipher and send it to another student to decode. The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the Polybius Square method. • Day 4 - In this lesson students will learn about the Vigenere Cipher. Students will receive an assignment that is encrypted using the Polybius Square Cipher. They have to solve the Polybius Square Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about the Vigenere Cipher. Students add an explanation about how the Vigenere cipher into their notebook. Students are broken up into groups and are asked to play the Crypto Go Card Game. Students are asked to encrypt a message using the Vigenere cipher about if they liked the game or not and send it to another student to decode. The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the Vigenere method. • Day 5 - In this lesson students will learn about the Four-Square Cipher. Students will receive an assignment that is encrypted using the Vigenere Cipher. They have to solve the Vigenere Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about the Four-Square Cipher. Students add an explanation about how the Four-Square cipher into their notebook. Students are asked to encrypt a message about what cipher they like best using the Four-Square cipher and send it to another student to decode.

	• Pen or Pencil • Crypto Go Card Game: González-Tablas Ferreres, A. I. and González Vasco, M. I. (2018). **Crypto Go: Symmetric key - English (open source) [Card game]**. Madrid: Universidad Carlos III de Madrid, Universidad Rey Juan Carlos. Available at http://hdl.handle.net/10016/28433 • Mission X-Code, from Amigo Games (available for purchase on Amazon) • *Pico CTF*, https://picoctf.com/ • Abelson, Ledeen, and Lewis. *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*. Addison-Wesley Professional, 2008.	The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the Four-Square method. • Day 6 - In this lesson students will learn about the Playfair Cipher. Students will receive an assignment that is encrypted using the Four-Square Cipher. They have to solve the Four-Square Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about the Playfair Cipher. Students add an explanation about how the Playfair cipher into their notebook. Students are then asked to complete at least one puzzle the cryptography room in Pico CTF. Students are asked to encrypt a message about what they learned in the puzzle they completed in the cryptography room in Pico CTF using the Playfair cipher and send it to another student to decode. The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the Playfair method. • Day 7 - In this lesson students will learn about Steganography. Students will receive an assignment that is encrypted using the Playfair Cipher. They have to solve the Playfair Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about Steganography in the Blown to Bits book - Hiding Information in Images (p. 95-99). Students add an explanation about Steganography into their notebook. Students are asked to encrypt a message in an image and send it to another student to decode. The students must turn in a copy of the encrypted message in the image and

		the plaintext. Students then must decode someone else's message hidden in an image.
4.3.1 LO: Students will define cryptography and explain how it is used in data security. EK: 4.3.1i,k 4.3.3 LO: Students will employ public key (asymmetric) encryption and explain how it works. EK: 4.3.3a,b,c,d 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. EK: 7.2.4f,g,h	• Notebook • "The Internet: Encryption & Public Keys." *YouTube*, uploaded by Code.org, 21 Aug 2015, https://www.youtube.com/watch?v=ZghMPWGXexs&feature=youtu.be • "CS Principles 2017 | Unit 4 | Ch. 1 | Lesson 7: Public Key Cryptography | Activity 1 | Activity Guide – Public Key Bean Counting." *Code.org*, https://docs.google.com/document/d/1l0KDF33-gWIssZGqfuHgD0QpF50Pdyqras46FeuNLgc/edit • Modulo Widget • Public Key Crypto Widget • "The Story of Digital Signatures and Public Key Infrastructure." *YouTube*,	**Understanding Public Key Encryption and Digital Signatures: (2-day lesson)** In this lesson students gain a better understanding of public key encryption through hands-on experiences and learn about how public key encryption relates to digital signatures. • This lesson begins with students watching a video about Encryption and Public Keys. Students take notes on the video in their notebook. They then gain hands-on experience in how public key encryption works through the Cups & Beans Activity from Code.org. Once the students experience this, they discuss what they have learned from the activity. Students then work with the Modulo Widget to have a better understanding of the math behind public key encryption followed by using the Public Key Crypto Widget with a partner to gain hands-on experience with public / private key encryption. The class discusses the experience with the widget. Students then watch the video on Digital Signatures and take notes in their notebook. After the video there is a class discussion on how digital signatures relate to public and private key encryption. Students then update their notebooks with the key vocabulary.

	uploaded by PKIIndia, 29 Apr 2016, https://www.youtube.com/watch?v=G7hs-3R86M0&feature=youtu.be	
4.3.3 LO: Students will employ public key (asymmetric) encryption and explain how it works. EK: 4.3.3a,b,c,d 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. EK: 8.1.2c	• Window Notes Sheet (access a blank Window Notes template at https://toolsforclassroominstructionthatworks.com/wp-content/uploads/2018/01/Window-Notes.pdf) • "The Evolution of Public Key Cryptography." *YouTube*, uploaded by NYU Tandon School of Engineering, 23 Oct 2018, https://www.youtube.com/watch?v=Pk-Hqsjq5HU&feature=youtu.be • Abelson, Ledeen, and Lewis. *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*. Addison-	**History & Politics of Public Key Encryption: (2-3-day lesson)** In this lesson students learn about the history of public key encryption and how government policies discouraged the use of encryption to build secure networks. • Students read p.165-193 in Blown to Bits. This reading includes topics such as Historical Cryptography and Lessons for the Internet Age. Students take window notes while reading. Following the reading, there is a class discussion about what students learned in the reading. Students then watch the video on the Evolution of Public Key Cryptography and take window notes. After the video the class discusses public key encryption and government policy. **Assessment:** *In groups of 3-4 students complete a breakout box using ciphers and steganography.*

	Wesley Professional, 2008.	

UNIT 6: NETWORKS, THE INTERNET, & IOT

Estimated Time in Hours: 24-27

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
1 Ethics 3 Ubiquitous Connectivity 5 System Security 6 Adversarial Thinking 7 Risk 8 Implications	1.1, 1.2, 3.1, 3.2, 5.4, 6.1, 7.2, 8.1	- Human Network - Build a Patch Cable - OSI Model Poster - Internet Widget (Code Lesson) - IOT Project - Detection System Presentation - Firewall Rules - Build Airgap Network

Guiding Questions:

- How is the Internet organized and what role do standards and protocols play in keeping networks secure?
- How does an adversary leverage connected networks to serve their purposes?
- How do network security technologies keep our systems and data secure?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
3.1.1 LO: Students will explain how devices use layers to communicate across the Internet and describe the purpose of the layers EK: 3.1.1a	• Notebook • Chart Paper • Yarn or String • "Computer Networks: Crash Course Computer Science #28." *YouTube*, uploaded by CrashCourse, 13 Sep 2017, https://www.youtube.com/watch?v=3QhU9jd03a0&feature=youtu.be • [D0X3D!] Game:	**Network Basics: (2-day lesson)** In this lesson students learn how a network is formed and how it works. • The lesson begins with a pre-assessment. Students brainstorm and list everything they know about networks on a piece of chart paper. Students are then put in groups of 5 - 7 students. The students are given a set of guidelines for a challenge to create a human network using the yarn or string. After the challenge, students reflect in their notebook on the strength of the network they developed and the weakness of the network they developed. Students then watch the Computer Networks video to understand what a network is and how it works.

	"Get the Game." [d0x3d!], *d0x3d.com*, https://d0x3d.com/d0x3d/get_the_game.html	Following the video, the class discusses how networks carry two types of information, those that allow for the controlling of the data and the data itself. Students then play the [D0X3D!] Game.
3.1.1 LO: Students will explain how devices use layers to communicate across the Internet and describe the purpose of the layers EK: 3.1.1b	• Notebook • "The Internet: Wires, Cables & Wifi." Uploaded by Code.org, 6 Oct 2015, https://www.youtube.com/watch?v=ZhEf7e4kopM&feature=youtu.be • Cat5e Cable • RJ45 Jacks • Crimper Tool • Cable Tester	**Understanding methods for sending data and the physical layer: (1-2-day lesson)** In this lesson students learn how data can move through the network by wires, cables, or WiFi and build a physical patch cable. • The lesson begins with students watching the video on Wires, Cables and WiFi. Following the video there is a discussion about how the wires, cables and WiFi are all a part of the physical layer. Students then build a physical cable. They follow the T-568B Wiring Standard. Once the students build the cable, it is tested using the cable tester to make sure it works properly. Students will use their cables later in the airgap network that they build later in the course. Students document the process of building the cable in their notebook and discuss the challenges they encountered.
3.1.1 LO: Students will explain how devices use layers to communicate across the Internet and describe the purpose of the layers EK: 3.1.1b,c,d,e,f 3.2.3 LO: Students will identify and distinguish between the	• Notebook • Window Notes Sheet (access a blank Window Notes template at https://toolsforclassroominstructionthatworks.com/wp-content/uploads/2018/01/Window-Notes.pdf)	**Understanding the Internet & OSI Model: (2-day lesson)** In this lesson students learn about how devices use layers to communicate across the internet and the purpose of the layers. • This lesson begins with a quick write. Students are asked the following questions: "What is the internet?" and "Is the internet the same thing as the World Wide Web?" Students share out their thoughts. Students watch The Internet video and The World Wide Web video. Students

purposes of network security devices and technologies. EK: 3.2.3a,b 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. EK: 7.2.4a,b 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. EK: 8.1.2a,b	• Poster Paper • "The Internet: Crash Course Computer Science #29." *YouTube*, uploaded by CrashCourse, 20 Sep 2017, https://www.youtube.com/watch?v=AEaKrq3SpW8&feature=youtu.be • "The World Wide Web: Crash Course Computer Science #30." *YouTube*, uploaded by CrashCourse, 4 Oct 2017, https://www.youtube.com/watch?v=guvsH5OFizE&feature=youtu.be • Shaw, Keith. "The OSI model explained: How to understand (and remember) the 7-layer network model." Network World, *NetworkWorld.com*, 22 Oct 2018, https://www.networkworld.com/article/3239677/the-osi-model-explained-how-to-understand-and-	take window notes during each video. After the videos, the class reflects on what they wrote during the quick write at the beginning of the hour and discusses what they have learned from the videos. The discussion is guided to the layers of the OSI model discussed in the video. After the discussion, students read the article on the OSI Model Explained. Students then create a poster of the OSI Model. The poster labels each layer, explains what the layer does, has an image to represent what happens at that layer and gives an example that the students learned from the videos. Students then play the Keeping Tradition Secure simulation. The lesson is wrapped up with a class discussion.

	remember-the-7-layer-network-model.html • "Keep Tradition Secure." Texas A&M University Division of Information Technology, https://keeptraditionsecure.tamu.edu/	
3.1.2 LO: Students will explain how network standards and protocols allow different types of devices to communicate. EK: 3.1.2a,b,c,d	• "CS Principles 2020-2021 | Unit 2 | Lesson 3: The Need for Addressing." *Code.org*, https://curriculum.code.org/csp-20/unit2/3/ • "The Internet: IP Addresses & DNS." *YouTube*, uploaded by Code.org, 10 Sep 2015, https://www.youtube.com/watch?v=5o8CwafCxnU&feature=youtu.be	**Need for Addressing: (1-day lesson)** In this lesson students learn about communication protocols and DNS. • In this lesson students learn about creating communication protocols through an unplugged scheduling activity. Students then use the internet simulator for the process. After the activity there is a class discussion and then the students watch the video on IP Addresses & DNS.
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. EK: 1.1.1c	• Notebook • KWL Chart (find example KWL chart at https://www.timvandevall.com/templates/kwl-chart-template/) • IOT Security & Privacy Podcast:	**Understanding IOT: (9 - 10-day lesson)** In this lesson students learn what IOT is and the security issues with IOT. Students program and interact with IOT devices. • This lesson begins with a pre-assessment using a KWL Chart, students identify what they know about the Internet of Things. Students then listen to the IOT Security & Privacy podcast using the Do You Hear What I

1.2.2 LO: Students will give examples of where/how tools are used in ways that were not intended by the system designer. EK: 1.2.2a,b 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. EK:5.4.1b,c,d 5.4.2 LO: Students will predict how physical systems that rely on software may be vulnerable to future attacks. EK: 5.4.2a,b,c,d,e,f,g 6.1.1 LO: Students will explain how cybersystems are complex systems. EK: 6.1.1a,b,c 6.1.2 LO: Students will explain how complexity impacts the failure of cybersystems.	Schneier, Bruce and Henage, Dan. "Crypto-Gram February 15, 2017." *The Crypto-Gram Security Podcast*, Libsyn, 15 Feb 2017, https://hwcdn.libsyn.com/p/7/8/c/78cf9bdc0d407209/crypto-gram-17-02.mp3?c_id=14318562&cs_id=14318562&destination_id=19374&expiration=1595269963&hwt=5a61155e604f4fac61c5c73593dea94e • IOT devices (micro:bits, arduino) • "BBC micro:bit | Combination Lock." Club Make, *TechWillSaveUs.com*, https://make.techwillsaveus.com/microbit/activities/combination-lock • Munro, Ken. "Internet of Things Security | TEDxDornbirn." *YouTube*, uploaded by TEDx Talks, 20 Sep 2018,	Hear strategy. Students are given a graphical organizer to capture their notes during this process. Students identify and discuss IOT devices they use on a daily basis and how those devices are used. The W section of the KWL chart is updated with questions that students have about IOT devices. Students are then split into 2 groups and each group is given a project with a different IOT device. One group completes a project with microbits (electronic safe), one group with arduinos (programming boebots with arduino). Once students complete the project they share out with the class. The class then discusses what they think the security issues are with the IOT projects they completed. Students then watch the IOT Security video or the IOT Helping or Harming video. The class discusses what they learned and added it to the KWL chart. Students then select an IOT device to research and write a report on that includes possible security issues.

EK: 6.1.2a,b,c,d,e 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. EK: 7.2.1a,b,c,d,e 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. EK: 8.1.2d,e,f,g	https://www.youtube.com/watch?v=pGtnC1jKpMg&feature=youtu.be • Barker, Rose. "Internet of Things: Are Smart Devices Helping or Harming? | TEDxSalem." *YouTube*, uploaded by TEDx Talks, 5 Apr 2018, https://www.youtube.com/watch?v=ipdTLJcIkWI&feature=youtu.be	
3.2.3 LO: Students will identify and distinguish between the purposes of network security devices and technologies. EK: 3.2.3c,d,f,g 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.	• Notebook • Window Notes Sheet (access a blank Window Notes template at https://toolsforclassroominstructionthatworks.com/wp-content/uploads/2018/01/Window-Notes.pdf) • Poster Paper • Textbook: Stallings, William and Brown, Lawrie. *Computer*	**Intrusion Detection, Firewalls and Intrusion Prevention Systems: (10-12-day lesson)** In this lesson students learn about Intrusion Detection, Firewalls, and Intrusion Prevention Systems. • Students read Chapter 8 in the textbook. After section 8.1, students create an intruders poster that has an image to represent each type of intruder and a definition next to the intruder. Students take Window Notes on section 8.2. & 8.3. Students are split up into 3 groups. Group 1 creates a presentation on section 8.4 - Host-Based Intrusion Detection, Group 2 creates a presentation on section 8.5 - Network-Based Intrusion Detection, and Group 3 creates a presentation on section 8.6 - Distributed or Hybrid Intrusion Detection. Each

EK: 7.2.4c,d,e	*Security: Principles and Practice, Third Edition*. Pearson, 2015. • Firewall Rules Worksheet • "Firewall PI." Cyber Pi Projects, *CyberPiProjects.com*, https://www.cyberpiprojects.com/cyber-security#/firewall-pi/ • Raspberry Pi	group then presents about their detection system. After section 8.7 students add key vocabulary into their notebooks. Students take Window notes on section 8.8 and 8.9. Students take a quiz on this chapter. • Students read Chapter 9 in the textbook and take window notes for each section. There is a class discussion on Firewalls and Intrusion Prevention Systems. Students complete a firewall rules worksheet. Students add key vocabulary from Chapter 8 & 9 in their notebook. The lesson is wrapped up with a discussion on risks with and how intrusion detection and prevention systems work. **Assessment:** *Students set-up a basic airgap network. They create a Firewall Pi and implement it in the airgap network.*

UNIT 7: HISTORY & ECONOMICS OF CYBER

Estimated Time in Hours: 6-8

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
5 System Security 6 Adversarial Thinking 8 Implications	5.2, 5.4, 6.1, 8.1, 8.2, 8.3	- Information Campaign Presentation - Phishing Simulation - Supply Chain Case Write-up - Targeted Attack Simulation

Guiding Questions:

- How have historical cybersecurity ideas and events impacted society?
- How has the expansion of the threat environment been addressed in society?
- How do risk management and economic trade-offs impact cybersecurity decisions?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
6.1.4 LO: Students will understand how social behaviors and human factors impact the cybersecurity of a system design. EK: 6.1.4a,b 8.1.1 LO: Students will summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field. EK: 8.1.1a,b,d 8.2.1 LO: Students will describe how political ideologies, economic structures, social	• Notebook • "How the Kim Dynasty Took Over North Korea | History." *YouTube*, uploaded by HISTORY, 27 Apr 2018, https://www.youtube.com/watch?v=56c6W8EGfcA&feature=youtu.be • Galante, Laura. "How (and why) Russia hacked the US election." *YouTube*, uploaded by TED, 25 May 2017,	**Information Campaigns: (1 - 2-day lesson)** In this lesson students learn how information campaigns were used and considered vital throughout history impacting the ruling family in a country and creating chaos in a US election. • The lesson begins with students brainstorming in their notebook, writing what they know about information campaigns and any campaigns they know about. Students then watch the video on the Kim Dynasty. There is then a class discussion about how the Kim Dynasty was put in place and has maintained power through an information campaign. Students go back to their notebook and reflect on what they have learned. Students then watch the video on How (and why) Russia Hacked the US election. The class discusses the video. After watching the video, students listen to the Influence Operation Kill Chain Podcast (stop at 17 min 40 sec). Students then discuss what they learned from the How

organizations, and cultural perceptions impact cybersecurity. EK: 8.2.1a,b	https://www.youtube.com/watch?v=TO-_kVIkY6A&feature=youtu.be • Operation Kill Chain Podcast (stop at 17 min 40 sec): Schneier, Bruce and Henage, Dan. "Crypto-Gram September 15, 2019." *The Crypto-Gram Security Podcast*, Libsyn, 15 Sep 2019, https://hwcdn.libsyn.com/p/5/f/a/5fad7065005f08b5/crypto-gram-2019-09.mp3?c_id=54940355&cs_id=54940355&destination_id=19374&expiration=1595269974&hwt=2283dfea4d63724de9cc5d77c5aa8c06	(and why) Russia Hacked the US election and the Influence Operation Kill Chain Podcast. Students then research information campaigns throughout history. They select a campaign and create a brief presentation on the campaign.
6.1.4 LO: Students will understand how social behaviors and human factors impact the cybersecurity of a system design. EK: 6.1.4a,b	• Notebook • Lord, Nate. "What is Social Engineering? Defining and Avoiding Common Social	**Social Engineering: (1-day lesson)** In this lesson students will learn how social engineering works and how it is used to design effective phishing attacks. • The lesson begins with the phishing video to introduce the topic. After the video the students reflect in their notebook about the strategy of social engineering used.

	Engineering Threats." Data Insider Blog, *DigitalGuardian.com*, 11 Sep 2018, https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats#:~:text=Social%20engineering%20is%20a%20non,into%20breaking%20standard%20security%20practices.&text=When%20successful%2C%20many%20social%20engineering,authorized%20access%20to%20confidential%20information. • Phishing Video: "It Wasn't Me - #SecureYourAccount." *YouTube*, uploaded by Dubai Police, 27 June 2019, https://www.youtube.com/watch?v=HTkdw	Students then read about social engineering. After reading about social engineering students watch a 3-minute video on a form of social engineering. The class then discusses social engineering. The lesson is wrapped up with students completing a phishing simulation.

	nwAqlg&feature=youtu.be • Social Engineering Video: "This is how hackers hack you using simple social engineering." *YouTube*, uploaded by oracle mind, 1 May 2016, https://www.youtube.com/watch?v=lc7scxvKQOo&feature=youtu.be • Phishing Simulation: "What is phishing?" Living Security, https://phishing.livingsecurity.com/	
8.3.3 LO: Students will describe how economics shape the decisions of consumers. EK: 8.3.3b,c	• "CS Principles 2017 | Unit 4 | Ch. 1 | Lesson 4: The Cost of Free." *Code.org*, https://curriculum.code.org/csp-1718/unit4/4/	**Consumers: (1-day lesson)** In the first day of the lesson students learn about how they have to give away their data in order to fully participate in today's economy. • Day 1 - Follow the Code.org "The Cost of Free" lesson.
5.2.2 LO: Students will know some common hardware-related vulnerabilities EK: 5.2.2a,b	• Notebook • Supply Chain Security & Trust Podcast:	**Supply Chain: (1-day lesson)** In this lesson students learn what a supply chain is, what the risks are and best practices to minimize the risks.

5.2.3 LO: Students will describe the process of developing secure hardware and validating that it is secure through its lifecycle. EK: 5.2.3a,b,c	Schneier, Bruce and Henage, Dan. "Crypto-Gram October 15, 2019." *The Crypto-Gram Security Podcast*, Libsyn, 15 Oct 2019, https://hwcdn.libsyn.com/p/1/4/1/141a42757fb7e7a1/crypto-gram-2019-10.mp3?c_id=56423036&cs_id=56423036&destination_id=19374&expiration=1595268544&hwt=a330ee278baf60848a9ff35ed7bb5bab • Soare, Bianca. "Supply Chain Cybersecurity: What Are the Risks?" Heimdal Security, 21 Jan 2020, https://heimdalsecurity.com/blog/supply-chain-cyber-security/ • Duca, Sean. "Supply chain remains the weakest link in cybersecurity." Supply	• The lesson begins with students listening to a podcast about supply chain security. Students then read about supply chains and take notes in their notebook. The class discusses the supply chain. Students then research and find a supply chain issue. Students complete a 1 page write up on the issue. They identify the issue, explain what happened, how it happened, and how it could be prevented in the future or ways to minimize the issue.

	Chain, *SupplyChainDigital.com*, https://www.supplychaindigital.com/technology/supply-chain-remains-weakest-link-cybersecurity • "Best Practices in Cyber Supply Chain Risk Management." National Institute of Standards and Technology Computer Security Resource Center, *CSRC.NIST.gov*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf	
8.1.1 LO: Students will summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field.	• Notebook • "'WEB WARRIORS' Documentary over cyber warfare." *YouTube*, uploaded by	**Cyber Warfare: (1-day lesson)** In this lesson students learn about cyber warfare and the impacts cyber warfare has on business and society. • The lesson begins with students completing a quick write in their notebook answering the following question:

EK: 8.1.1c,f,h 8.2.1 LO: Students will describe how political ideologies, economic structures, social organizations, and cultural perceptions impact cybersecurity. EK: 8.2.1a,b	Techofriendly, 18 Nov 2016, https://www.youtube.com/watch?v=0IY7DL0ihYI&feature=youtu.be	"What is cyber warfare?" Students then watch the "Web Warriors" video. Students take notes on the video. The lesson wraps up with a class discussion about cyber warfare.
8.2.1 LO: Students will describe how political ideologies, economic structures, social organizations, and cultural perceptions impact cybersecurity. EK: 8.2.1d,e 8.3.1 LO: Students will explain how misaligned incentives encourage businesses to under invest in cybersecurity. EK: 8.3.1a,b,c,d 8.3.2 LO: Students will explain how economic forces influence the cybersecurity choices made by service providers and service designers. EK: 8.3.2a,b,c,d	• "Targeted Attack: The Game." Trend Micro, http://targetedattacks.trendmicro.com/ • Notebook	**Business Experience Simulation: (1-2-day lesson)** In this lesson students walk through a business simulation where they will have to make the proper choices based on the information given in order to avoid a successful cyber attack against the company. • The lesson begins with students being introduced to the Targeted Attack simulation. Students work through the simulation, making decisions about how to address cyber issues while maintaining the budget and keeping the project on target. Once students complete the simulation they reflect in their notebook what went right or wrong. If they failed the simulation, they can go back through it to see where they made mistakes. The class is wrapped up with a discussion about the standards addressed in this lesson.

8.3.3 LO: Students will describe how economics shape the decisions of consumers. EK: 8.3.3a,d		

UNIT 8: SECURE SOFTWARE

Estimated Time in Hours: 10-13

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
5 System Security 7 Risk	5.3, 5.4, 7.1, 7.2	- Software Vulnerability Discussion - Buffer Overflow Coding Problems - Hacker Game - Pico CTF Web Exploits

Guiding Questions:

- What are security flaws/vulnerabilities in software?
- Why does software have security vulnerabilities?
- What are the consequences of less secure software?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
5.3.1 LO: Students will describe common security-related software vulnerabilities. EK: 5.3.1a,b,c,d 7.1.4 LO: Students will be able to conduct standard security testing and assessments. EK: 7.1.4e 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	• "Hackers & Cyber Attacks: Crash Course Computer Science #32." *YouTube*, uploaded by CrashCourse, 18 Oct 2017, https://www.youtube.com/watch?v=_GzE99AmAQU&feature=youtu.be • Podcast (stop at 4 min 40 sec): Schneier, Bruce and Henage, Dan. "Crypto-Gram February 15, 2020." *The Crypto-Gram*	**What is secure software & why do we care? (1-2-day lesson)** In this lesson students learn about software security issues. • The lesson begins with students completing a quick write in their notebook answering the following question: "What are the consequences of less secure software?" The lesson is then introduced: Today we will be learning about software security issues and identify why we care about the issues. The students watch the Hackers & Cyber Attacks Video and take Cornell notes on the video. After the video, students add key vocabulary from the video into their notebook. The class has a brief discussion about what was learned from the video (be sure to address risks: vulnerabilities in databases, ethical hacking and software updates). Students then listen to the podcast linked left (listen from the beginning of the podcast to 4 min 40 sec). The class has a brief discussion about what they learned in the podcast (be sure to

rather than the system's original objective. EK 7.2.3a,b,c	*Security Podcast*, Libsyn, 15 Feb 2020, https://hwcdn.libsyn.com/p/4/f/f/4ff722d465bd469f/crypto-gram-2020-02.mp3?c_id=66980507&cs_id=66980507&destination_id=19374&expiration=1595268380&hwt=86c49be2206efbe3d3f1fb4e659470f4 • Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Notebook • Cornell Notes (for an explanation of the Cornell note-taking system, visit http://lsc.cornell.edu/study-skills/cornell-note-taking-system/) • Hacker: Cybersecurity Logic Game, by ThinkFun	discuss how software changes could come from an adversary and how changes in software code from an adversary can be difficult to detect). Students play the Hacker Board game in pairs. Students then read Section 11.1 (Software Security Issues) p.358 - 362 in the textbook and take notes. The lesson is wrapped up with students answering Review Question 11.1.

	(available for purchase on Amazon)	
5.3.1 LO: Students will describe common security-related software vulnerabilities. EK: 5.3.1b 5.3.2 LO: Students will identify the processes of developing secure software. EK: 5.3.2b	• Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Notebook • Cornell Notes (for an explanation of the Cornell note-taking system, visit http://lsc.cornell.edu/study-skills/cornell-note-taking-system/)	**Understanding Buffer Overflow: (4-5-day lesson)** In this lesson students learn about buffer overflow. • The lesson begins with students completing a quick write in their notebook answering the following question: "Why does software have security vulnerabilities?" Students popcorn their responses. Students read chapter 10 in the textbook and take Cornell notes on the chapter. As the students are reading they update the vocabulary in their notebook. Students complete chapter 10 review questions 10.1, 10.2, 10.5, & 10.9 and problems 10.2, 10.3, 10.4, 10.5, 10.10, and 10.11.
5.3.1 LO: Students will describe common security-related software vulnerabilities. EK: 5.3.1a,b,c,d,e,f 5.3.2 LO: Students will identify the processes of developing secure software. EK: 5.3.2a,b,c,d	• Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Notebook • Cornell Notes (for an explanation of the Cornell note-taking system, visit http://lsc.cornell.edu/stu	**Understanding Software Security: (5-6-day lesson)** In this lesson students learn about software security - handling input, writing safe program code, interacting with the operating system and other programs, and handling program output. • The lesson begins with students completing a quick write in their notebook answering the following question: "What are security flaws / vulnerabilities in software?" Students share their response with a partner. On person from each pair shares out. Students read chapter 11 in the textbook and take Cornell notes on the chapter. As students are reading, they update the vocabulary in their notebook. Students answer the following chapter 11

	dy-skills/cornell-note-taking-system/) • *Pico CTF*, https://picoctf.com/	review questions: 11.1, 11.3, 11.4, 11.5, 11.6, 11.13 & 11.16. **Assessment:** *Students complete the Web Exploit room in PicoCTF.*

UNIT 9: SECURITY AND VULNERABILITIES

Estimated Time in Hours: 23 - 30

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 3 Ubiquitous Connectivity 4 Data Security 5 System Security 6 Adversarial Thinking 7 Risk	2.1, 2.2, 2.3, 3.1, 3.2 ,4.2, 5.2, 5.3, 6.1, 6.2, 7.1, 7.2,	- Cyber Real Card Game - Create a Threat, Vulnerability, Attack Game - Attack Tree Poster - Create an Authentication Game - Security Vulnerability Table - Physical Controls Diagram - DoD Cyber Awareness Challenge - NIST Poster

Guiding Questions:

- How are simplicity and restriction overarching ideas for cybersecurity principles?
- What are security flaws/vulnerabilities in hardware and software?
- What is the difference between a risk, vulnerability, and a threat?
- How is cybersecurity risk modeled?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
2.2.1 LO: Students will explore the principle of simplicity, which is about how users can easily translate their general protection goals to appropriate system security configurations. EK: 2.2.1a,b,c 2.2.2 LO: Students will use the principle of abstraction to represent complicated concepts more simply and to allow	• Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Notebook • Introduction to Cybersecurity First Principles Lesson: Hale, Ghandi, Morrison, and Rausch.	**Fundamental Security Design Principles: (2-3-day lesson)** In this lesson students learn the fundamental security design principles. • Day 1 of the lesson: The lesson begins with students responding to the following question in their notebook: "What do you need to think about when designing a secure system?" Students then read section 1.4 - Fundamental Security Design Principles (p.17 - 21) in the textbook. Students take window notes as they are reading and update key vocabulary from this section in their notebook.

solutions to be transferred to other contexts. EK: 2.2.2a,b 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. EK: 2.2.3a,b,c,d 2.3.1 LO: Students will explore the principle of domain separation, which allows for the enforcement of rules governing the entry and use of domains by entities outside the domain. EK: 2.3.1a,b 2.3.2 LO: Students will know that the principle of process isolation prevents tampering or interference from/by other processes. EK: 2.3.2a,b,c 2.3.3 LO: Students will know that the principle of resource encapsulation allows access or manipulation of the resource only in intended ways.	"Introduction to Cybersecurity First Principles." *GitHub*, uploaded by mlhale, https://mlhale.github.io/nebraska-gencyber-modules/intro_to_first_principles/README/#cybersecurity-first-principles • Cyber Realm Card Game: https://gencybercards.com/ • GenCyber First Principles: https://users.cs.jmu.edu/tjadenbc/Bootcamp/0-GenCyber-First-Principles.pdf • First Principles using pictures: https://spark.adobe.com/page/DbZGSqJ12Q82A/ • First Principles Hand Gestures: https://gencyber.utulsa.edu/wp-content/uploads/2016/10/10-Principles-	• Day 2+ of the lesson: This lesson uses the Introduction to Cybersecurity First Principles Lesson. Students read the First Principles, followed by the CIA Triad Expectations, and then students play the Cyber Realm Card Game. The lesson is wrapped up with a quiz.

EK: 2.3.3a,b 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. EK: 2.3.4a,b,c 2.3.5 LO: Students will explore 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. EK: 2.3.5a,b 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. EK: 2.3.6a	GenCyber-Card-Game.pdf	

2.3.7 LO: Students will recognize that the principle of modularity is a design technique that separates the functionality of a program into independent components. Each component is self-sufficient and capable of executing a unique part of the desired functionality through well-designed interfaces. EK: 2.3.7a,b 2.3.8 LO: Students will explore the principle of fail-safe defaults, which restricts how privileges are initialized when a subject or object is created. EK: 2.3.8a,b,c 5.2.4 LO: Students will identify hardware security addresses issues related to an adversary physically gaining access to a device. EK: 5.2.4a,b		
7.1.1 LO: Students will be able to differentiate between threats, vulnerabilities, and attacks. EK:7.1.1a,b,c	• Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015.	**Understanding Threats, Vulnerabilities, and Attacks: (2-day lesson)** In this lesson students learn the difference between threats, vulnerabilities, and attacks. • The lesson begins with a quick write. Students answer the following question: "What is the difference between

	• Notebook	an attack, a threat, and a vulnerability?" Students then read section 1.2 - Threats, Attacks, and Assets (p.9-15) and A Model for Computer Security (p.7-8) in the textbook. Students update the vocabulary in their notebook. In small groups students create a game that will help others to practice identifying threats, vulnerabilities and attacks.
4.2.3 LO: Students will evaluate and recommend technical controls that can be used to secure data. EK: 4.2.3a,b,c,d,e,j	• Notebook • Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015.	**Authentication / Securing Data: (5-6-day lesson)** In this lesson students learn about all of the different ways to secure data with authentication. • Day 1: Students read section 3.1 - Digital User Authentication Principles (p.64-70) in the textbook. Students update the key vocabulary in their notebook. Students answer Review Question 3.1. • Day 2: Students read section 3.2 - Password-Based Authentication (p.70-82) in the textbook. Students update the key vocabulary in their notebook. Students answer Review Questions 3.2,3.3 & 3.4. Students complete Problems: 3.1 & 3.3. • Day 3: Students read section 3.3 - Token-Based Authentication (p.82-87) in the textbook. Students update the key vocabulary in their notebook. Students answer Review Question 3.5. • Day 4: Students read section 3.4 - Biometric Authentication (p. 87 - 92) in the textbook. Students update the key vocabulary in their notebook. Students answer Review Questions 3.6 & 3.7. • Day 5+: Student read section 3.5 - Remote User Authentication, and 3.6 - Security Issues for User Authentication (p.92-97) in the textbook. In pairs

		students create a game to review the types of authentication.
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. EK: 3.2.2a,b,c,d	• Holl, Kim. "SANS Security Essentials | GSEC Practical Assignment Version 1.4b | OSI Defense in Depth to Increase Application Security." Global Information Assurance Certification, *GIAC.org*, https://www.giac.org/paper/gsec/2868/osi-defense-in-depth-increase-application-security/104841#:~:text=Many%20of%20the%20threats%20to,flooding%20and%20spanning%20tree%20attacks. • Notebook	**OSI Vulnerabilities: (1-day lesson)** In this lesson students identify and predict outcomes of security vulnerabilities at the different layers of the OSI Model. • The lesson begins with students reviewing and diagramming the layers of the OSI model in their notebook. Students then read the OSI Defense in Depth paper. While reading the document students fill out a table that includes the following: vulnerability, layer, outcome.
2.1.3 LO: Students will evaluate methods of protecting information and information systems from disruption and destruction. EK: 2.1.3d	• "Beta – Hotspot Game." Living Security | Resources | Intelligence Center | Games, https://hotspot.livingsecurity.com/	**Physical Security: (3-4-day lesson)** In this lesson students identify physical controls that are used to secure data. • The lesson begins with students completing the Hot Spot Hunt for the Violations simulation. After students complete the simulation the class discusses what violation(s) is/are physical security violation(s). Students

4.2.2 LO: Students will identify physical controls that are used to secure data. EK: 4.2.2a,b,c,d,e,f 6.1.3 LO: Students will understand how different system components impact the cybersecurity of a system design. EK: 6.1.3a,b,c,d 6.2.1 LO: Students will know how natural events and unintentional errors can cause a system to fail. EK: 6.2.1a,b,c,d	• Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Notebook • Cornell Notes (for an explanation of the Cornell note-taking system, visit http://lsc.cornell.edu/study-skills/cornell-note-taking-system/) • "Cyber-Physical Systems." UC Berkeley Electrical Engineering and Computer Sciences Dept. Ptolemy Project, https://ptolemy.berkeley.edu/projects/cps/#:~:text=Cyber%2DPhysical%20Systems%20(CPS),affect%20computations%20and%20vice%20versa.	then read section 16.1- Overview, 16.2- Physical Security Threats, 16.3 - Physical Security Prevention and Mitigation Measures, and 16.4 - Recovery From Physical Security Breaches (p.508-519) & 16.6 - Integration of Physical and Logical Security (p. 520 - 526) in the textbook. Students take Cornell notes as they are reading. Students add key vocabulary to their notebooks. Students answer Review Questions 16.8. Then, students read Cyber-Physical Systems. The lesson is wrapped up with students creating a diagram explaining physical controls used to secure data.
5.2.2 LO: Students will know some common hardware-related vulnerabilities. EK: 5.2.2c,d,e	• Bhunia, Swarup and Tehranipoor, Mark. "Side-Channel Attacks." *Hardware Security: A*	**Side Channel Attacks: (1-day lesson)** In this lesson students learn how hardware may act in unintended ways due to side channel attacks.

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. EK: 7.2.3c,d	*Hands-On Learning Approach*, Morgan Kaufmann, 2 Nov 2018, pp. 193-218. • Notebook	• In this lesson students read about side channel attacks. They take notes on the reading. The lesson is wrapped up with students discussing the vulnerabilities of hardware and how to secure the hardware.
5.3.3 LO: Students will describe the process of validating that software remains secure through its lifecycle. EK: 5.3.3a,b,c,d,e 7.1.4 LO: Students will be able to conduct standard security testing and assessments. EK: 7.1.4a,c,d,e	• Gonzalez, Kenneth. "A Step-By-Step Guide to Vulnerability Assessment." Security Intelligence, *SecurityIntelligence.com*, 8 June 2018, https://securityintelligence.com/a-step-by-step-guide-to-vulnerability-assessment/ • "What is a Zero-Day Exploit?" Fire Eye, *FireEye.com*, https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html • Notebook	**Testing & Security:(3-4-day lesson)** In this lesson students learn how to validate that software remains secure through its lifecycle. • The lesson begins with a quick write answering the question: "What is a Zero Day Exploit?". Students respond in their notebooks. The lesson is then introduced and students read about zero-day exploits and the step by step guide to vulnerability assessment. The class then discusses the process of validating software through its lifecycle. Students create a poster representing the process for validating the software. In the next part of the lesson, students learn what is necessary to conduct standard security testing and assessment. • Begin with a discussion about vulnerability assessments and how they play a part in standard security testing. Students then read Application Security Best Practices - Top 10 Checklist. The class then discusses each of the topics on the checklist. Students then apply what they

	• Poster Paper • Markers • Avner, Gabriel. "Application Security Best Practices Top 10 Checklist." White Source | Resources | Blog, 1 Aug 2019, https://resources.whitesourcesoftware.com/blog-whitesource/application-security-best-practices • Control-Alt-Hack, by Steven Jackson Games (available for purchase on Amazon or at controlalthack.com)	know about standard security testing and assessments through the game Control-Alt-Hack.
6.2.2 LO: Students will know how intentional attacks can adapt to defenses and cause a system to fail. EK: 6.2.2a,b,c,d 7.1.2 LO: Students will be able to identify and prioritize the	• "The Cybersecurity Framework Version 1.1 Downloadable Presentation." National Institute of Standards & Technology, *NIST.gov*, Oct 2019, https://www.nist.gov/document/cybersecuri	**NIST: (3-4-day lesson)** In this lesson students learn about the NIST Framework and how to apply the NIST Framework to a situation. • The lesson begins with students reading section 1.6 - Computer Security Strategy (p.24-26) in the text. Students take Cornell notes while reading. The teacher then introduces the NIST Framework with the NIST Framework PowerPoint. Students then read the NIST Framework documentation and take notes in their

protection of information assets. EK: 7.1.2a,b,c	tyframeworkv1-1presentationpptx • "Framework Version 1.1 (PDF)- Framework for Improving Critical Infrastructure Cybersecurity." National Institute of Standards & Technology, *NIST.gov*, 16 Apr 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf • Cornell Notes (for an explanation of the Cornell note-taking system, visit http://lsc.cornell.edu/study-skills/cornell-note-taking-system/) • Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Notebook • Poster Paper • Markers	notebook. The class discusses how the NIST Framework works and they walk through a model NIST Framework together. Students will then work in groups to create their own NIST Framework poster to protect a set of assets.

3.1.2 LO: Students will explain how network standards and protocols allow different types of devices to communicate. EK: 3.1.2e,f,g 7.1.3 LO: Students will create a threat model and evaluate the trade-offs associated with defending against different threat sources. EK: 7.1.3a,b,c 7.1.5 LO: Students will understand the trade-offs between cybersecurity benefits and the total cost of cybersecurity protections. EK: 7.1.5a,b,c 7.2.2 LO: Students will be able to describe how the presence of an adversary necessitates that cybersecurity risk is emergent and complex. EK: 7.2.2a,b,c 7.2.4 LO: Students will be able to explain how the decentralized and dynamic nature of networked systems create the	• Notebook • Textbook: Stallings, William and Brown, Lawrie. *Computer Security: Principles and Practice, Third Edition*. Pearson, 2015. • Schneier, Bruce. "Attack Trees." Schneier on Security, *Schneier.com*, https://www.schneier.com/academic/archives/1999/12/attack_trees.html • Poster Paper • Markers	**Attack Trees: (1-2-day lesson)** In this lesson students learn about attack trees and identify a possible asset and create an attack tree for the asset. • The lesson begins with a class brainstorming session about attack trees. "Attack trees" is written in the center of the board and students list all of the things they know about attack trees. Each idea is connected to the word. Students then read section 1.5 - Attack Surfaces and Attack Trees (p.21-24) in the textbook. Students then read the Attack Tree Examples. The class then goes back to the attack trees brainstorming list. They cross out any misconceptions that are listed and add the brainstorm to their notebook. Students are then put in small groups. Each group receives a poster paper. The group picks a target and creates an attack tree for the target.

potential for a system to fail or behave incorrectly due a component the designer didn't even know existed. EK: 7.2.4i		
3.2.1 LO: Students will analyze how the connected nature of the Internet allows an adversary to reach a large number of devices. EK: 3.2.1a,b,c,d 6.2.3 LO: Students will analyze how the cybersecurity attack lifecycle/kill chain is essential to adversarial thinking. EK: 6.2.3a,b,c,d,e,f,g,h	• Hospelhorn, Sarah. "What is The Cyber Kill Chain and How to Use it Effectively." Varonis Blog, *Varonis.com*, 29 Mar 2020, https://www.varonis.com/blog/cyber-kill-chain/ • "Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform." Lockheed Martin, 2015, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf • Degonia, Tony. "Explaining the Cyber Kill	**Kill Chain: (2-3-day lesson)** In this lesson students will analyze how the cybersecurity attack lifecycle / kill chain is essential to adversarial thinking. • A diagram of the Cyber Kill Chain is introduced to the students at the beginning of the lesson. Students read about the Cyber Kill Chain. Students create a diagram of the Kill Chain that labels each part of the kill chain and explains how each part works. Students are then given a scenario where they analyze how the connected nature of the internet allows an adversary to reach a large number of devices and they apply the kill chain to the scenario. The lesson is wrapped up with students applying what they have learned about the kill chain to stop a breach in the DoD Cyber Awareness Challenge 2020.

	Chain Model." AT&T Business | AT&T Cybersecurity, 3 Jan 2019, https://cybersecurity.att.com/blogs/security-essentials/the-internal-cyber-kill-chain-model • "Cyber Awareness Challenge 2020", sponsored by the Department of Defense Chief Information Office (DoD CIO), https://dl.dod.cyber.mil/wp-content/uploads/trn/online/cyber-awareness-challenge/launchPage.htm	