HIGH SCHOOL CYBERSECURITY CURRICULUM GUIDELINES & GLOSSARY

As Of
2/5/2021

Table of Contents

Big Idea #1 – Ethics

Cybersecurity has broad implications. Ethical reflection and judgement are required to make decisions about the trade-offs between the benefits and harms. Whether a system's design or the use of the system constitutes a benefit or harm depends on the ethical duties and interests of both the designer and user. Designers and users can have differing interests when it comes to deciding what is worth protecting and which cybersecurity resource investments are justified to achieve that protection. All cybersecurity exists within a context of social, organizational, and personal values; these values undergird beliefs about right and wrong. In this course, students will have the opportunity to evaluate the ethical implications among all stakeholders.

Essential Questions:

- What is an ethical way to disclose vulnerabilities?
- 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?

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
1.1: Social goals reflect the foundational values held by society; these core societal values are reflected in cybersecurity choices.	1.1.1: 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.	1.1.1a: Societies are groups of individuals characterized by common interests/values that are perpetuated by persistent social interaction.
		1.1.1b: Cybersecurity ethics is an expression of values by the designers and users.

	1.1.1c: Values concerning how to engage in cyber technologies can and do compete during the creative process of designing the technology and its adoption.
	1.1.1d: Different communities and societies have different foundational social goals and values that impact their behaviors concerning technology.
1.1.2: Students will understand how the role of values and ethics affects political structures, laws, and policy decisions as it relates to cybersecurity.	1.1.2a: 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: Institution refers to informal norms, shared understandings, and formal doctrines that constrain and prescribe actors' interactions with one another.
	1.1.2c: Cyberwarfare, cybersecurity and privacy affect and are affected by institutions, political structures and policies.
	1.1.2d: Cybersecurity laws reflect values about national security, economic security, welfare of citizens, domestic law and order, and legitimacy of government.
	1.1.2e: Professional codes of ethics convey the expected conduct of cybersecurity professionals.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
1.2: Ethical reflection and judgement are required in considering the potential harms, benefits, and trade-offs involved in cybersecurity.	1.2.1: Students will discuss how cybersecurity can significantly impact the quality of people's lives both positively and negatively.	1.2.1a: Examples in history demonstrate the harms and benefits of cybersecurity from multiple perspectives.
		1.2.1b: 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: Cybersecurity requires resources, including time, money, and expertise that also affects technological affordances.
	1.2.2: Students will give examples of where/how tools are used in ways that were not intended by the system designer.	1.2.2a: 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: 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.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
1.3: Cybersecurity practices are highly complex and variable causing tensions between what the ethical duties are, to whom the ethical concern should be considered, and whose interests should be invested in protecting.	1.3.1: Students will explore the tensions that exist between transparency, autonomy, resilience and security.	1.3.1a: Transparency is important for trustworthiness and openness in a society, but can come at a risk to privacy and security.
		1.3.1b: Autonomy means that every entity is in control of their own thoughts and actions.
		1.3.1c: Resilience is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.
		1.3.1d: Security is freedom from potential harm or other unwanted coercive change caused by others.
	1.3.2: Students will discuss how ethical obligations to society always coexist with ethical obligations to one's family, friends, employer, local	1.3.2a: Ethical obligations are covenants that define a moral course of action and draw a line between right and wrong.

community, and even oneself.	
	1.3.2b: 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.
1.3.3: Students will discuss how even when a cybersecurity practice is legal, it may not be ethical.	1.3.3a: The legal and ethical consequences of cybersecurity practices can be explored through ethical versus malicious (e.g., white/gray/black hat) hacking.
	1.3.3b: Technology moves faster than laws can be created to govern it.
	1.3.3c: Using the anonymity of the internet for behavior that can harm others may not be illegal.
	1.3.3d: Disclosure of software vulnerabilities to a party other than the software developer is legal and can be harmful.

Big Idea #2 - Establishing Trust

Knowledge of the fundamental cybersecurity principles is necessary to determine security requirements and mechanisms, as well as to identify vulnerabilities and threats. The principles derive from the ideas of simplicity and restriction. Understanding the related assumptions is also important in considering the strength of a system's security. This course emphasizes the cybersecurity principles, the CIA triad and how to question assumptions as the basis for establishing trust in cybersecurity. Students in this course evaluate the principles and apply them to systems creating trust within organizations.

Essential Questions:

- How are confidentiality, integrity, and availability interconnected?
- What is essential for establishing trust in cybersecurity?
- How are simplicity and restriction overarching ideas for cybersecurity principles?
- How do we know a system is well-defended?

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
2.1 Cybersecurity relies on confidentiality, integrity, and availability (the CIA triad).	2.1.1: Students will evaluate methods of keeping information secret from those whom the information should be kept secret.	2.1.1a: Confidentiality is the protection of information from disclosure to unauthorized parties.
		2.1.1b: File permissions are a mechanism to control access to only those authorized.
		2.1.1c: Cryptography is necessary to ensure confidentiality and integrity.
		2.1.1d: Hiding is another aspect of confidentiality.

	2.1.1e: Assuring confidentiality includes prevention, detection, and response mechanisms.
2.1.2: Students will demonstrate that integrity involves trust and credibility.	2.1.2a: Integrity is the trustworthiness of data or resources.
	2.1.2b: Assurance is determining how much and in which way to trust a system.
	2.1.2c: Data integrity is the information changing in authorized ways by authorized people, often called authentication.
	2.1.2d: Integrity mechanisms include prevention, detection and response mechanisms.
2.1.3: Students will evaluate methods of protecting information and information systems from disruption and destruction.	2.1.3a: Availability of information refers to ensuring that authorized parties are able to access the information when needed.
	2.1.3b: Denial of service attacks are attempts to block availability
	2.1.3c: There is a tradeoff between 1) confidentiality and integrity and 2) availability.

		2.1.3d: Assuring availability includes prevention, detection, and response mechanisms.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
2.2: The simpler you can make the design or implementation of a system, the better you can check whether or not it can be exploited.	2.2.1: Students will describe the principle of simplicity, which is about ensuring that systems are easy to understand, maintain and test so as to be more secure.	2.2.1a: Simple designs are easier to understand, maintain and test for security problems.
		2.2.1b: Simplicity is also known as “Economy of Mechanism.”
		2.2.1c: A simple design incorporates a careful analysis of what is needed.
	2.2.2: Students will use the principle of abstraction to represent complicated concepts more simply and to allow solutions to be transferred to other contexts.	2.2.2a: Abstraction is reducing the complexity of an object down to its essentials in a way that is understandable.
		2.2.2b: Good and elegant design involves using abstraction.

	2.2.3: Students will apply the principle of minimization by decreasing the number of ways in which attackers can exploit a program or device.	2.2.3a: The attack surface of a software environment is the sum of the different points where an unauthorized user can try to enter data or to extract data from an environment.
		2.2.3b: Minimizing the attack surface decreases the opportunity to find an exploitable vulnerability in the system.
		2.2.3c: The human interface should be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.
		2.2.3d: Common mechanisms and access should be minimized.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
2.3: The more you restrict access, processes, resources, and users based on the policy, the more secure the system.	2.3.1: Students will give examples of the principle of domain separation, which allows for the enforcement of rules governing the entry and use of domains by entities outside the domain.	2.3.1a: A domain refers to a collection of data or instructions that warrant protection.

	2.3.1b: Communications between domains are allowed only as authorized.
2.3.2: Students will explain that the principle of process isolation prevents tampering or interference from/by other processes.	2.3.2a: A process is a program running on a computer.
	2.3.2b: Each process has a region of the memory (address space), which only it can access.
	2.3.2c: Processes have to use defined communications mediated by the operating system to communicate with other processes.
2.3.3: Students will explain the importance of encapsulating resources, i.e., creating well-defined interfaces around resources to set rules for how the resources should interact.	2.3.3a: Examples of resources are the memory, disk drive, network bandwidth, battery power, and a monitor. It can also be system objects such as shared memory or a linked list data structure.
	2.3.3b: Encapsulation allows access or manipulation of the class data in only the ways the designer intended.

2.3.4: Students will define 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.	2.3.4a: A privilege is a right for the user to act on managed computer resources.
	2.3.4b: 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: Granting only those privileges necessary for a user to accomplish assigned duties improves accountability and limits accidental misuse.
2.3.5: Students will break down how the principle of layering is a strategy for slowing down an attack because the attacker has to conquer	2.3.5a: A layer is a separate level that must be conquered by an attacker to breach a system.

each layer before moving on to the next.	
	2.3.5b: Multiple independent layers require integration and independent management to get the full benefits of layered protection.
2.3.6: 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.	2.3.6a: Data hiding can help prevent users/programmers/processes from updating/changing data in invalid ways or by mistake.
2.3.7: Students will recognize that cybersecurity often applies to a system that consists of individual self-sufficient components and the overall security is dependent on the security prosperities of the components.	2.3.7a: The principle of modularity says that individual components are capable of executing a unique part of the desired functionality and is achieved through system design. Because of this modular design, security upgrades can happen in one component without having to overhaul the entire system.
	2.3.7b: A system's components may be separated and recombined.

	2.3.8: Students will define the principle of fail-safe defaults, which restricts how privileges are initialized when a subject or object is created.	2.3.8a: When something does not work or the system fails, the system must return to a secure state.
		2.3.8b: A secure state is a condition when no subject can access any object in an unauthorized manner.
		2.3.8c: Turning off permission causes a security problem.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
2.4: Identifying and questioning assumptions is a key part of making a system more secure.	2.4.1: Given a scenario, students will identify the assumptions made in the design of the system, evaluate their impact on security, and consider how different assumptions change the security.	2.4.1a: 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: 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: Incorrect assumptions lead to system failures.
	2.4.1d: When confronting incorrect assumptions, facing up to cyber attacks is an ongoing, and constantly evolving challenge.
	2.4.1e: The only assumption you can safely make is that data and networks are not safe.

Big Idea #3: Ubiquitous Connectivity

Networks are used daily by most people in the world. There is no single network but rather a collection of different network technologies that together form a network of networks called the Internet. Conceptually, the Internet is divided into layers with protocols and standards that define each layer. This enables a large variety of devices to be connected. This vast number of devices connected over a large number of network technologies is referred to as ubiquitous connectivity. In other words, everything is connected all the time. The more dependent we become on ubiquitous connectivity, the greater the implications if the network becomes compromised. This makes it necessary for students to understand and effectively use the methods and tools for keeping our network secure.

Essential 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?

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
3.1: The Internet is a large, globally distributed network that is divided into layers, governed by protocols, and connects a wide variety of devices.	3.1.1: Students will explain how devices use layers to communicate across the Internet and describe the purpose of the layers.	3.1.1a: Networks carry two types of information, those that allow for the controlling of the data and the data itself.
		3.1.1b: 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: 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.
	3.1.1d: The network layer connects different types of networks to form larger networks and ultimately the global Internet. It transmits data from one computer to another using packets and logical addressing.
	3.1.1e: 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: Internet and device applications (web, text messaging, games, etc.) follow protocols at the application layer (e.g. http, sms, proprietary protocols, etc.).
3.1.2: Students will explain how network standards and protocols allow different types of devices to communicate.	3.1.2a: 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: One commonly used protocol is the Domain Name System (DNS) which provides a mechanism to map names like “www.example.com” into numbers (IP addresses), similar to a phonebook that maps names to phone numbers.

		3.1.2c: 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: Some standards are open standards where the packet format and message exchange rules are available to everyone. In other standards called proprietary standards, the message formats and message exchange rules are only provided to authorized entities.
		3.1.2e: When designers rely on secrecy, assuming an adversary cannot compromise the system because the adversary cannot determine how the system works is known as security through obscurity. It is widely accepted that security through obscurity should never be your only security mechanism.
		3.1.2f: Cryptographic algorithms are either publicly known or proprietary. The use of proprietary cryptographic algorithms is largely discredited, as evidenced by organizations like NIST, which encourages public review of algorithms.
		3.1.2g: Through experiments, an adversary can often learn how proprietary protocols or algorithms work even though the adversary is not an authorized user.

Enduring Understanding	**Learning Objectives**	**Essential Knowledge Statements**

3.2: The Internet provides a large attack surface, which offers efficiencies or economies of scale for adversaries.	3.2.1: Students will analyze how the connected nature of the Internet allows an adversary to reach a large number of devices.	3.2.1a: 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: 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: An adversary can attack a large number of systems simultaneously, which can impact a large majority of a group of people.
		3.2.1d: An adversary can stay undetected for a long period of time suggesting that early detection is key in preventing a large amount of damage.
	3.2.2: 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.	3.2.2a: 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: At the network layer, an adversary may do two things, impersonate an address (spoofing) or disrupt communication (Denial of Service).
	3.2.2c: 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: 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.
3.2.3: Students will identify and distinguish between the purposes of network security devices and technologies.	3.2.3a: 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: 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: Firewalls work primarily at the network and transport layer by blocking packets with addresses and ports that correspond to unwanted traffic.
	3.2.3d: 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: Intrusion Prevention Systems (IPS) are similar to IDS and also can prevent attacks by blocking messages related to anomalies or signatures.
	3.2.3f: Application layer defenses, such as input validation, check and block potentially harmful message data from getting to the application.
	3.2.3g: 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.

Big Idea #4: Data Security

Data is all around us; keeping it secure and private is essential for individuals, groups, and governments. The concept of what data is, and how it can be collected, has changed monumentally with the advent of the Internet. With an ease of collection created by improved computing power, data can be generated, stored, transmitted, and manipulated at a much greater pace and at an almost immeasurable amount. Keeping those with malicious intent away from data assets and preserving privacy is a major tenet in Cybersecurity. Because data can tell us so much about our world, it is important to keep the confidentiality, integrity, and availability of the data intact. Students in this course will study relevant laws and policies governing data; evaluate the tools used to connect cyber-physical systems; and practice using the encryption techniques needed to secure data across networks.

Essential Questions:

- What actions can be taken to validate that data has been unaltered by an unauthorized source?
- What policies and procedures are in place to keep data safe?
- How is the integrity of data being transported over networks safeguarded?
- What are the ways in which data can be encrypted?
- Why is privacy essential for individuals, groups, and governments?

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
4.1: 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.	4.1.1: Students will analyze existing data security concerns and assess methods to overcome those concerns.	4.1.1a: Data can reveal much about people, their thoughts, and lives; which makes personally identifiable information highly sensitive.
		4.1.1b: Data can be used to help individuals, but it can also be exploited to harm individuals.

		4.1.1c: Data must be protected in processing, transmitting and storage.
		4.1.1d: 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: Data integrity means only authorized changes are made only by authorized people.
		4.1.1f: Origin integrity means the original data is trustworthy, and its source is trusted to produce trustworthy data.
		4.1.1g: Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
4.2: Data Security uses non-technical and technical controls and techniques to protect data that is being processed, transmitted and stored.	4.2.1: 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.	4.2.1a: Policies can be introduced and enforced at the local, state, and national levels.

	4.2.1b: Laws are in place to protect the disclosure and misuse of financial, personal, and private information.
	4.2.1c: GDPR (General Data Protection Regulation) is a set of regulations designed to give citizens in the European Union more control over their personal data.
	4.2.1d: HIPAA (Health Insurance Portability and Accountability Act) is United States legislation that provides data privacy and security provisions for safeguarding medical information.
	4.2.1e: CFAA (Computer Fraud and Abuse Act) prohibits accessing a computer without authorization, or in excess of authorization.
	4.2.1f: There are also state cybersecurity laws. One example are the Data Breach Disclosure laws that exist in 48 states, but differ by state. Another example is CCPA (California Consumer Privacy Act), which was signed into law in 2018 to extend the privacy rights of the citizens of California.
	4.2.1g: 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.
4.2.2: Students will identify physical controls that are used to secure data.	4.2.2a: Physical security controls are means and devices to control physical access to sensitive information and to protect the availability of the information.

	4.2.2b: Physical security is an important part of defense in depth. To provide comprehensive physical security, multiple systems and processes must work together, like perimeter security, access control, and process management.
	4.2.2c: Commonly used physical controls include: limited entry points, redundant systems, and surveillance cameras.
4.2.3: Students will evaluate and recommend technical controls that can be used to secure data.	4.2.3a: Authentication is a process by which you verify that someone is who they claim they are.
	4.2.3b: Authentication requires a database of information.
	4.2.3c: Authentication can be done using multiple factors, something you have, something you know, something you do, and something you are. (E.g., have = card, know=password, do=sign, walk, are=fingerprint, retina)
	4.2.3d: Identity management includes authentication, access control, sometimes coordination across different domains, and management of the credentials throughout the lifecycle.
	4.2.3e: Passwords and passphrases are a common form of authentication.

		4.2.3f: The strength of a password is a function of length, complexity, and unpredictability.
		4.2.3g: 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: Groups, Roles, Privileges and Permissions are used to manage authorization.
		4.2.3i: Access Control is the process of enforcing the required security for a particular resource.
		4.2.3j: Failure to protect data can be due to faulty authentication, faculty authorization, and/or faulty access control.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
4.3: Cryptography techniques are necessary to keep data private and secure, and evolve with changes in technology.	4.3.1: Students will define cryptography and explain how it is used in data security.	4.3.1a: Cryptography comes from two Greek words meaning "secret writing" and is the art and science of concealing meaning.
		4.3.1b: Cryptanalysis is the breaking of codes.

	4.3.1c: Cryptographic algorithms, also known as ciphers, which are mathematical functions used in the process of encryption and decryption.
	4.3.1d: 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: 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: Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result.
	4.3.1g: The primary goal of cryptography is to keep enciphered information secret.
	4.3.1h: Symmetric encryption is a method of encryption involving one key for encryption and decryption.
	4.3.1i: Public key encryption, which is asymmetric, is an encryption method that is widely used because of the enhanced security associated with its use.
	4.3.1j: Hash functions can be used for checking whether a file was corrupted.

	4.3.1k: Certificate authorities (CAs) issue digital certificates that validate the ownership.
4.3.2: Students will practice symmetric cryptosystems to send a message and explain how they work.	4.3.2a: 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: 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: Anagramming is a way to attack a transposition cipher. It uses tables of n-gram frequencies to identify common n-grams.
	4.3.2d: A substitution cipher changes characters in the plaintext to produce the ciphertext.
	4.3.2e: A shift cipher is susceptible to a statistical ciphertext-only attack.
4.3.3: Students will employ public key (asymmetric) encryption and explain how it works.	4.3.3a: Public key encryption does not require the sender and receiver to share the same key.

	4.3.3b: 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: 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: Digital Signatures are a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate.

Big Idea #5: System Security

This big idea addresses security flaws and vulnerabilities in hardware and software.
Hardware and software work together to achieve an objective. Adversaries may exploit weaknesses in the system to disrupt the systems confidentiality, integrity, or availability. System security includes definitions and explanations of security flaws and vulnerabilities, helps explain why hardware and software have vulnerabilities, introduces students to some specific vulnerabilities, and addresses the consequences of less secure hardware and software.

Essential Questions:

- How do hardware and software work together to achieve an objective?
- What are security flaws/vulnerabilities in hardware and software?
- Why do hardware and software have security vulnerabilities?
- What are the consequences of less secure hardware and software?

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
5.1: Systems consist of a combination of hardware and software that together achieve some objective and security requires integration of both.	5.1.1: Students will identify how hardware and software work together in complex ways to achieve an overall objective.	5.1.1a: Software is a set of instructions that execute on hardware and are designed to achieve some objective on a physical device.
		5.1.1b: Neither hardware or software is useful without the other.
		5.1.1c: 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.
	5.1.1d: Malware, short for malicious software, is any software intentionally designed to cause damage to a computer, server, client, or computer network.
	5.1.1e: 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: 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: 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: 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: 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: 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.
		5.1.1k: 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 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: 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.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
5.2: Hardware security protects the machine and peripheral hardware from theft and from electronic intrusion and damage.	5.2.1: Students will convey that computer hardware refers to the physical parts of a computer and related devices.	5.2.1a: Internal hardware devices include CPUs, motherboards, hard drives, memory, and internal peripherals such as a CD-ROM drive, CD-R drive, or internal modem.

	5.2.1b: External hardware devices include monitors, keyboards, mice, printers, scanners, routers, switches, servers, IoT devices industrial control systems, and security cameras.
	5.2.1c: Hardware is the base level component of systems that are critical to telecommunications, health, US economic system, and national defense.
	5.2.1d: 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.
5.2.2: Students will identify some common hardware-related vulnerabilities.	5.2.2a: 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: Manufacturing backdoors are used for malware or other penetrative purposes; backdoors aren't limited to software and hardware, but they also affect embedded radio-frequency identification (RFID) chips and memory.
	5.2.2c: A side channel attack is based on information gained from the use of an algorithm or computer system, rather than weaknesses in the algorithm itself (e.g. cryptanalysis and software bugs).

	5.2.2d: General classes of side channel attacks include attacks such as: timing attacks, power-monitoring attacks, electromagnetic attacks, data remanence attacks.
	5.2.2e: Hardware vulnerabilities can also be due to weaknesses in the implementation of algorithms.
5.2.3: Students will describe the process of developing secure hardware and validating that it is secure through its lifecycle.	5.2.3a: 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: The hardware design, manufacturing and supply chain can be attacked by malicious actors, nation states, competitors, and organized crime.
	5.2.3c: Physical security measures can be used to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm.
5.2.4: Students will identify hardware security issues related to an adversary physically gaining access to a device.	5.2.4a: The hardware design can require the device to disable itself if physically tampered with.

		5.2.4b: Students will identify examples of fail-safe in cybersecurity, i.e., a design feature or practice that in the event of a specific type of failure, inherently responds in a way that will cause no or minimal harm to other equipment, the environment or to people, and provide recovery opportunities.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
5.3: 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: Students will describe common security-related software vulnerabilities.	5.3.1a: 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: 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: 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: 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: Changes to the environment can cause software to no longer meet the security policy and secure software must include considerations for how to implement future changes (e.g., credentials, algorithms, and patching code to correct bugs and errors).
	5.3.1f: A software vulnerability can occur when external components that don't meet the security policy requirements are connected to the system.
5.3.2: Students will identify the processes of developing secure software.	5.3.2a: 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: 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: Development tools and Integrated software Development Environments (IDE)s provide static analysis tools to check for some types of insecure code such as identifying potential buffer overflows.
5.3.3: Students will describe the process of	5.3.3a: A security analysis is a process that is used to verify a program meets a specified list of security requirements.

validating that software remains secure through its lifecycle.		
		5.3.3b: Security vulnerability reports such as Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE) are publicly available for software systems and should be monitored, or subscribe to their alerts.
		5.3.3c: A zero-day vulnerability is a software security flaw that is unknown to people who should be responsible for patching or fixing the flaw. Zero-day attacks are cyber attacks utilizing one or multiple zero-day vulnerabilities.
		5.3.3d: Managing vulnerability reports, patching and patch distribution is a key part of software security.
		5.3.3e: Dynamic analysis is a process in which external tools analyze the execution of code in order to automatically identify potential security vulnerabilities.

Enduring Understanding	**Learning Objectives**	**Essential Knowledge Statements**
5.4: Software and Hardware (or Systems) are everywhere which increasingly makes it	5.4.1: Students will identify historical consequences of software and hardware vulnerabilities, e.g.,	5.4.1a: 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).

foundational in civilization.	power outages, death, theft of trade secrets from other sovereign nations.	
		5.4.1b: 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: 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: 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).
	5.4.2: Students will predict how physical systems that rely on software may be vulnerable to future attacks.	5.4.2a: 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: Industries that employ CPS include energy management, health care, manufacturing, transportation, telecommunications, infrastructure, and military.
	5.4.2c: A smart grid is an electrical grid which includes a variety of operation and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficient resources.
	5.4.2d: Increased industry connectivity will cause increased attacks from adversaries such as cyber criminals, disgruntled employees, terrorists, organized crime, and nation states.
	5.4.2e: Vulnerabilities may allow adversaries to interfere with connected devices.
	5.4.2f: The consequences of unintentional faults or malicious attacks could have severe impact on human lives and the environment.
	5.4.2g: By targeting trusted resources attackers can control devices and wholeheartedly manipulate users.

Big Idea #6: Adversarial Thinking

A primary objective of cybersecurity is to identify critical assets, design and implement systems to protect the assets, identify ways to detect when the protections fail, respond to the failures, and ultimately recover to a working state. To accomplish this, one must think about what can go wrong. This big idea extends the concept of adversary to anything that might disrupt the system, from a clever cybercriminal who will adapt to a natural disaster. Students will learn to consider how an adversary might attempt to find key assets, compromise those assets, and avoid detection. The most challenging adversaries adapt to defenses and adjust their attacks based on the system's responses. Students in this course will challenge assumptions and practice thinking about opposing forces, in terms of intentions (when opposing forces are human adversaries), capabilities, and actions. Students will employ these techniques to analyze threats and vulnerabilities, as well as attacks.

Essential Questions:

- How are systems disrupted by both intentional attacks and unintentional events?
- How does a cybersecurity life cycle/kill chain capture how an adversary approaches compromising a system?
- How is the presence of opposing forces considered when creating a system's defense?

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
6.1: Adversity comes from anyone or anything where the end result differs from that intended by the system designer and user.	6.1.1: Students will explain how cybersystems are complex systems.	6.1.1a: A complex system is a system composed of many components which may interact with each other.
		6.1.1b: Complex systems typically have input from many sources and are highly changeable.

	6.1.1c: 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.
6.1.2: Students will explain how complexity impacts the failure of cybersystems.	6.1.2a: In complex systems, failures are rarely the result of one individual's problem or behavior; catastrophe requires multiple failures.
	6.1.2b: 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: 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: Given the complexity of cybersystems, there are limits to how much entities can control their functioning and success of their policies.
	6.1.2e: Security is a characteristic of systems and not system components.
6.1.3: Students will identify and explain how different system components impact the	6.1.3a: Security is only as strong as the weakest link and is not limited to human actors.

	cybersecurity of a system design.	
		6.1.3b: Human operators have dual roles: as producers and defenders against failure.
		6.1.3c: Events ranging from natural disasters to unintentional errors can result in cybersecurity failures.
		6.1.3d: Change introduces new forms of failure.
	6.1.4: Students will understand how social behaviors and human factors impact the cybersecurity of a system design.	6.1.4a: Human users of the system have their own conscious and unconscious objectives that can undermine cybersecurity protections and policies.
		6.1.4b: 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.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements

6.2: Adversarial thinking is the process of reasoning about how opposing forces could prevent a system from meeting both its functional and security goals.	6.2.1: Students identify the ways in which natural events and unintentional errors can cause a system to fail.	6.2.1a: Cyber systems are susceptible to disruption and destruction from natural disasters; for example, flooding, earthquakes, and hurricanes.
		6.2.1b: Disaster planning includes provisioning for the confidentiality, integrity and availability of cyber systems during natural disasters.
		6.2.1c: Disaster planning includes prevention, detection, and response and recovery.
		6.2.1d: Natural event and unintentional errors typically do not adapt in response to defenses.
	6.2.2: Students will explain how intentional attacks can adapt to defenses and cause a system to fail.	6.2.2a: The intentions of adversaries can be classified as theft, disclosure, disruption, destruction, and/or subversion.
		6.2.2b: 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: Cyber systems are susceptible to attack from human adversaries.

	6.2.2d: Incident response includes provisioning for the confidentiality, integrity and availability of cyber systems under attack by adversaries.
6.2.3: Students will analyze how the cybersecurity attack lifecycle/kill chain is essential to adversarial thinking.	6.2.3a: The term “kill chain” refers to the structure—or seven stages—of a cyberattack.
	6.2.3b: Reconnaissance is the first stage in the attack lifecycle, where adversaries gather public information about the target, and scan their networks to identify how best to plan their attack.
	6.2.3c: Weaponization is the second stage. Based on the information obtained through reconnaissance, the adversary will tailor their toolset to meet the specific requirements of the target network. This often includes coupling remote access with an exploit into a deliverable payload.
	6.2.3d: The third phase is delivery, which is the transmission of the weapon to the target environment using vectors like email attachments, phishing, websites, and removable media.
	6.2.3e: Exploitation is the fourth phase where the code is triggered exploiting vulnerable applications or systems.
	6.2.3f: The fifth stage is installation where attackers install a remote access trojan or backdoor on the victim system in order to conduct

	further operations, such as maintaining access, persistence and escalating privileges.
	6.2.3g: Command and control is the sixth phase of the cyber kill chain. With malware installed, attackers now own both sides of the connection: their malicious infrastructure and the infected machine and can now actively control the system. Attackers will establish a command channel in order to communicate and pass data back and forth between the infected devices and their own infrastructure.
	6.2.3h: The final stage of the kill chain is actions on the objective. Once adversaries have control, persistence, and ongoing command and communication, they will act upon their motivation in order to achieve their goal(s), e.g., data exfiltration, destruction of critical infrastructure, to deface web property, or to create fear or the means for extortion.

Big Idea #7 Risk

Risk, as defined in regards to cybersecurity, is a relationship between the chance that some harm will occur and the damage that will be done if it does occur. This big idea engages students in this course with the risk assessment process as a methodology for grasping cybersecurity risk. This big idea also addresses the inherently uncertain and complex nature of cybersecurity risk due to complexity of systems of systems, the presence of adversaries, the logical malleability of computing, and the dynamic and distributed nature of computing.

Essential Questions:

- What is the difference between a risk, vulnerability, and a threat?
- How is cybersecurity risk modeled?
- How does the presence of an adversary contribute to the complexity of cybersecurity risk?
- How does the logical malleability of computers contribute to the complexity of cybersecurity risk?
- How does the dynamic, distributed, and ubiquitous nature of computing contribute to the complexity of cybersecurity risk?

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
7.1: Cybersecurity risk is a measure of the potential damage or loss a vulnerability could cause weighed against the likelihood an adversary will exploit the vulnerability.	7.1.1: Students will be able to differentiate between threats, vulnerabilities, and attacks.	7.1.1a: 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: A threat is anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.
		7.1.1c: Attacks arise when threats exploit vulnerabilities.
	7.1.2: Students will be able to identify and	7.1.2a: Information assets must be identified.

prioritize the protection of information assets.	
	7.1.2b: 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: 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.
7.1.3: Students will create a threat model and evaluate the trade-offs associated with defending against different threat sources.	7.1.3a: Threats originate from internal (insider) and external sources such as nation states, multinational criminal organizations, and hacktivists/terrorists.
	7.1.3b: Bad actors in cyberspace are characterized by their resources, capabilities/techniques, motivations, and aversion to risk.
	7.1.3c: There are risks and solutions associated with closed/proprietary systems.
7.1.4: Students will be able to conduct standard security	7.1.4a: Vulnerability assessment identifies known vulnerabilities on the system.

testing and assessments.	
	7.1.4b: Known vulnerabilities can be found in databases that collect, maintain, and disseminate information.
	7.1.4c: There are various automated vulnerability scanning tools, which are used for pinpointing vulnerabilities and providing remediation for these vulnerabilities.
	7.1.4d: Not all vulnerabilities can be exploited and not all vulnerabilities need to be mitigated.
	7.1.4e: Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.
7.1.5: Students will understand the trade-offs between cybersecurity benefits and the total cost of cybersecurity protections.	7.1.5a: The outcome of a risk assessment should prioritize what needs to be remediated.
	7.1.5b: 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: The level of protection is a function of the attack occurring and the effects of the attack should it succeed.
Enduring Understanding	**Learning Objectives**	**Essential Knowledge Statements**
7.2: 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.	7.2.1: 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.	7.2.1a: 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: 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: The behavior or output of cybersystems cannot be predicted simply by analyzing the parts and inputs of the system.
		7.2.1d: 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: 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.
7.2.2: Students will be able to describe how the presence of an adversary necessitates that cybersecurity risk is emergent and complex.	7.2.2a: Adversaries employ strategic reasoning, including where, when, and how they might attack, as well as tactics for evading detection.
	7.2.2b: The steps in an attack are footprinting, scanning, enumeration, network mapping, gaining access, privilege escalation, implant, and hiding tracks.
	7.2.2c: Adversaries are self-interested agents whose behavior evolves and adapts in response to their environments and other actors in the system.
7.2.3: Students will be able to explain how the logical malleability of software and hardware can allow an adversary to change a system to	7.2.3a: Software is frequently updated to correct both functional errors and security problems.

meet the adversary's goals rather than the system's original objective.	
	7.2.3b: Software changes could come from an adversary that intentionally inserts code to meet the goals of the adversary.
	7.2.3c: Changes in software code are common and those introduced by an adversary are often not easily detected.
	7.2.3d: Hardware itself may act in unintended ways and an adversary is seeking to find and exploit these unintended behaviors.
7.2.4: 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.	7.2.4a: There are risks and mitigations associated with open systems like the Internet.
	7.2.4b: 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: 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: Network vulnerabilities can result in the loss of integrity if data is sent to an imposter acting as a "man-in-the-middle" or when data is sent over a path where it can be changed.
	7.2.4e: Network vulnerabilities can result in the loss of availability by directing the sender to an invalid destination or sending data over a path where it can be dropped.
	7.2.4f: Cryptography can be used to prevent imposters and protect data so only authorized entities can view it.
	7.2.4g: Cryptography can be used to identify the creator of a message and show a message was not modified in transit (hash function).
	7.2.4h: Certificate authorities play a role in asserting the identities.
	7.2.4i: Cryptography does not solve operational challenges and cryptography alone is not a solution in a decentralized network.

Big Idea #8: Implications

Advances and decisions at a local level in computing, connectivity, and big data are driving a global, interconnected phenomenon and have significant cybersecurity implications. Societies face cybersecurity issues regarding infrastructure, law enforcement, and social and cultural issues. Economic concerns and risk management trade-offs drive decisions that significantly impact cybersecurity. Cybersecurity is shaped by critical historical ideas and events. History proves that adversaries can launch attacks from anywhere transcending global borders, requiring adaptation. This course differentiates between the severity of cyber threats and stresses the fact that threats evolve along with the technology which enables the adversary to evolve with their attacks. Students in this course describe historical events and their cybersecurity implications examining the evolution of the threat environment at the local and global level.

Essential 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?

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
8.1: Cybersecurity shapes and is shaped by significant historical ideas and events.	8.1.1: Students will summarize and interpret the impact of cybersecurity ideas and events on the evolution of the field.	8.1.1a: Information campaigns were used and considered vital throughout history.
		8.1.1b: 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: Events in cyber warfare and cybercrime escalated the need for increased cybersecurity efforts.
	8.1.1d: The loss of confidentiality is a critical factor in warfare.
	8.1.1e: The violation of system integrity can alter the behavior of critical infrastructure.
	8.1.1f: A loss of availability has disrupted critical business functions.
	8.1.1g: The emergence of advanced persistent threats (APTs) have caused changes in the way individuals and companies are secured and who is involved in securing them.
	8.1.1h: 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.
8.1.2: Students will explain how the idea of the open internet led us to new innovations that impact our daily lives and our security.	8.1.2a: The Internet provides global connectivity and is not structured around national boundaries.
	8.1.2b: Security was not seen as a concern until much of the “infrastructure” for computer networks was in place.

		8.1.2c: Early government policies discouraged the use of encryption to build secure networks.
		8.1.2d: The Internet has evolved to include new types of devices and the “Internet of Things."
		8.1.2e: 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: The Internet and IoT devices create new vulnerabilities an adversary can exploit.
		8.1.2g: The increasing dependence on the Internet and IoT devices introduces problems when these systems become unavailable.
		8.1.1h: 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.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
8.2: Cybersecurity is global, transcending traditional boundaries, and is always evolving.	8.2.1: Students will describe how political ideologies, economic structures, social organizations, and	8.2.1a: Nation states have various approaches to sovereignty, investment and deterrence regarding cyber technology.

cultural perceptions that impact cybersecurity.	
	8.2.1b: Cybersecurity is impacted by the state of a political alliance between nation states.
	8.2.1c: Past and current laws are insufficient to assign blame for taking action that make our systems more vulnerable or to punish an entity for cyber crimes.
	8.2.1d: To ensure the safety of a nation's critical infrastructure both public and private sectors are responsible for cybersecurity.
	8.2.1e: Depending on the values of the entity, some will invest in research and development, while others invest in reverse engineering the work of others.
	8.2.1f: Citizens in cyber space can more readily form ideological communities which is impacting what it means to be a nation state.
	8.2.1g: Cultural perceptions and priorities of security may differ between countries affecting how and which security measures are implemented.
8.2.2: Students will analyze how privacy concerns vary greatly	8.2.2a: Nation states have various approaches to civil rights and privacy regarding cyber technology.

	in regards to societies, age, and socio-economic status.	
		8.2.2b: 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: When a government provides cybersecurity it can often lead to the reduction of privacy.

Enduring Understanding	Learning Objectives	Essential Knowledge Statements
8.3: Measuring the economic value of cybersecurity is often an indirect process that relies on risk management trade-offs rather than direct benefits.	8.3.1: Students will explain how misaligned incentives encourage businesses to under invest in cybersecurity.	8.3.1a: Economic value typically measures gains achieved, not losses avoided.
		8.3.1b: 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: The lack of cybersecurity can result in major financial and reputational loss, but this loss only occurs after a successful attack.

	8.3.1d: Even in the event of a successful attack, the loss may or may not have lasting direct economic impact on the provider of the service.
	8.3.1e: When misaligned incentives arise the party making the security–efficiency trade-off is not the one who loses out when attacks occur.
8.3.2: Students will explain how economic forces influence the cybersecurity choices made by service providers and service designers.	8.3.2a: 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: 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: Cybersecurity risks occur when outsourcing the production or maintenance of technology to third party sources that may have different security practices.
	8.3.2d: 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.

8.3.3: Students will describe how economics shape the decisions of consumers.	8.3.3a: 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: 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: 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: 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.

Glossary

A

Abstraction In cybersecurity, abstraction refers to the act of simplifying complex security systems by breaking them down into essential pieces, wherein each piece should have its own security capabilities.

Access Control The process of granting or denying specific requests: for obtaining and using information and related information processing services; and to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). (4)

Advanced Persistent Threat (APT) An adversary with sophisticated levels of expertise and significant resources. The APT pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives. (1)

Adversary An entity that is not authorized to access or modify information, or who works to defeat any protections afforded the information. (4)

Algorithm A set of step-by-step, detailed instructions used to solve a problem or perform a calculation.

Alternate Site A backup facility that has the necessary electrical and physical components of a computer facility.

Anomaly Abnormality or deviation.

Application A software program hosted by an information system. (1)

Application Layer An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network. This layer interacts with software applications that implement a communicating component. (5)

Asymmetric Cryptography Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation. (1)

Attack Signature A specific sequence of events indicative of an unauthorized access attempt. (1)

Authentication Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (1)

Authorization The granting or denying of access rights to a user, program, or process. (4)

Availability Ensuring timely and reliable access to and use of information. (4)

B

Backdoor An undocumented way of gaining access to computer system. A backdoor is a potential security risk. (1)

Backup A copy of files and programs made to facilitate recovery, if necessary. (1)

Blacklist A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity. (1)

Boundary Physical or logical perimeter of a system. (1)

Buffer Area of a computer's memory designated to hold data.

Buffer Overflow A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. (1)

C

Central Processing Unit (CPU) The component of a computer system that performs the basic operations (such as processing data) of the system, that exchanges data with the system's memory or peripherals, and that manages the system's other components. (3)

Certificate A data structure that contains an entity's identifier(s), the entity's public key and possibly other information, along with a signature on that data set that is generated by a trusted party, i.e. a certificate authority, thereby binding the public key to the included identifier(s). (4)

Certificate Authority: A trusted entity that issues and revokes public key certificates. (4)

Cipher Series of transformations that converts plaintext to ciphertext using the Cipher Key. (1)

Ciphertext: Data in its encrypted form.

Common Vulnerabilities and Exposures (CVE) A nomenclature and dictionary of security-related software flaws. (1)

Common Weakness Enumeration (CWE) A taxonomy for identifying the common sources of software flaws (e.g., buffer overflows, failure to check input data). (1)

Confidentiality The protection of information from disclosure to unauthorized parties. Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.

Credential Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once. (1)

Cryptanalysis The breaking of coded messages.

Cryptography From two Greek words meaning "secret" and "writing", the process of concealing the meaning of transmitted information.

Cyberspace The online world of computer networks and especially the Internet (3)

Cybersystems - Cybersystems are the complex environment existing in digital form which include the people, software, services, and devices typically connected via a large or small network.

D

Data Remanence Attack Data remanence is residual information remaining on storage media even after attempts have been made to remove or erase the data. An attack that exploits data remanence can disclose sensitive information.

Decryption The process of transforming ciphertext into plaintext using a cryptographic algorithm and key. (4)

Denial of Service (DoS) When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests. (2)

Disaster Recovery Plan (DRP) A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. (1)

Distributed Denial of Service (DDoS) A denial of service technique that uses numerous hosts to perform the attack. (1)

Dynamic Analysis: The process of detecting software vulnerabilities by executing the program and analyzing the program's behavior.

E

Edge Network A network located on the periphery of a centralized network.

Electromagnetic Attack In cryptography, electromagnetic attacks are side-channel attacks performed by measuring the electromagnetic radiation emitted from a device and performing signal analysis on it. (5)

Encryption The process of changing plaintext into ciphertext.

Enumeration Organizing information such as user names, machine names, network resources, shares and services found in the information gathering step of an attack.

Escalating Privileges Privilege escalation, entails the exploitation of a bug or flaw that allows for a higher privilege level than what would normally be permitted. (4)

F

Firewall Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorized access to or from a network. (2)

Footprinting Footprinting, aka reconnaissance, refers to the techniques used for gathering information about computer systems and the entities to whom they belong to be used by an attacker to gain access to the target's resources.

H

Hard Drive A data-storage device consisting of a drive and one or more hard disks. (3)

Hardware The physical parts of a computer and related devices.

Hashing The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. (1)

Hypertext Transfer Protocol (HTTP) HTTP is a protocol typically used by web browsers and web servers. It defines how messages are formatted and transmitted and actions that should be taken in response to various commands.

Hypertext Transfer Protocol Secure (HTTPS) The HTTPS protocol encrypts HTTP data being sent back and forth with encryption, so that if someone were to capture the data being transferred via HTTPS, it would be unrecognizable.

I

Implant Electronic device or electronic equipment modification designed to gain unauthorized interception of information-bearing emanations. (1)

Input Validation Processes added to the program which verifies that input provided by an external source is the type of input expected and will be processed correctly.

Integrated Development Environment (IDE) A software application that provides comprehensive tools to computer programmers for software development. (5)

Integrity A property possessed by data items that have not been altered in an unauthorized manner since they were created, transmitted or stored. (5)

Interface Common boundary between independent systems or modules where interactions take place. (1)

Internet of Things (IoT) Internet of things describes both the physical and virtual things and the networks they use to function.

Intrusion A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so. (1)

Intrusion Detection The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents. (1)

Intrusion Detection System (IDS) Software that automates the intrusion detection process. (1)

Intrusion Prevention The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents. (1)

Intrusion Prevention System (IPS) System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. (4)

IP Address An IP (Internet Protocol) address is a numerical label assigned to each computer which uses the Internet Protocol to communicate over a network.

K

Kill Chain The structure or stages an adversary moves through in a cyberattack.

L

Link Layer (i.e., Data Link Layer) The data link layer is the protocol to establish and terminate a connection between two physically connected devices, as well as controlling the flow between the devices.

M

Man in the Middle Attack An active attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them. (4)

Memory A device (such as a chip) or a component of an electronic device (such as a computer or smartphone) in which information can be inserted and stored and from which it may be extracted when wanted. (3)

Motherboard The main circuit board especially of a microcomputer. (3)

N

N-Gram In computational linguistics, n-gram refers to a contiguous sequence of n words from a sample of text.

Network Layer The network layer provides the protocol for transferring variable length data sequences (i.e., packets) from a source to a destination via one or more networks.

Network Mapping A process that discovers, collects, and displays the physical and logical information required to produce a network map. (4)

P

Packet A block of data transmitted over a network.
Patch An update to firmware or software to improve security and/or enhance functionality. (2)

Patching Applying updates to firmware or software to improve security and/or enhance functionality. (2)

Perimeter Security Establishing techniques or functional methods at the perimeter of a network to secure data and resources.

Permission Authorization to perform some action on a system. (4)

Personally Identifiable Information Information which, when used alone or in conjunction with other information, can be used to identify an individual. Common examples of personally identifiable information include social security numbers, birth dates, images and addresses.

Physical Layer The physical layer provides protocol for the transmission and reception of data over physical transmission medium such as an ethernet cable, optical cable, or wireless channel.

Power-Monitoring Attack A type of side channel attack in which a malicious actor monitors power consumption by a device's hardware during computation.

Private Key A cryptographic key used with an asymmetric-key (public-key) cryptographic algorithm that is not made public and is uniquely associated with an entity that is authorized to use it. (4)

Privilege A right granted to an individual, a program, or a process. (1)

Privilege Escalation (see **Escalating Privileges**)

Public Key A cryptographic key used with an asymmetric-key (public-key) cryptographic algorithm that may be made public and is associated with a private key and an entity that is authorized to use that private key. (4)

Public Key Cryptography (i.e., Asymmetric Encryption) Encryption system that uses a public-private key pair for encryption and/or digital signature. (4)

Protocol A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. (1)

R

Ransomware Malicious software that makes data or systems unusable until the victim makes a payment. (2)

Redundancy A secondary system or device which can take over operation should the main system/device fail.

Remote Access Trojan A remote access Trojan (RAT) is a malicious computer program that lets a remote adversary access your computer and control it.

Risk A measure of the potential damage or loss a vulnerability could cause weighed against the likelihood an adversary will exploit the vulnerability.

Router A network device which sends data packets from one network to another based on the destination address. May also be called a gateway. (2)

S

Shift Cipher The shift cipher s a kind of substitution cipher. When using a shift cipher, each letter of the plaintext is replaced by a letter "x" number of positions down the alphabet.

Side Channel Attack An attack enabled by leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions. (4)

Software A set of instructions that execute on hardware and are designed to achieve some objective on a physical device. Software instructions may manipulate data, manipulate physical systems or manipulate both.

Static Analysis: The process of detecting software vulnerabilities by examining the program's code and attempting to reason over all possible behaviors without actually executing the program.

Substitution Cipher A substitution cipher is a method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system. (5)

Symmetric Cryptography (i.e. Symmetric Encryption) Encryption algorithms using the same secret key for encryption and decryption. (4)

T

Threat Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Timing Attack A type of side channel attack in which the attacker attempts to discover vulnerabilities and to compromise a cryptosystem by studying the time it takes that system to execute cryptographic algorithms.

Transport Layer The transport layer is the protocol responsible for reliable connection-oriented or connectionless end-to-end communications.

Transposition Cipher A transposition cipher is a method of encryption in which units of plaintext are rearranged, according to a fixed system, without making any substitutions.

Trojan A type of malware or virus disguised as legitimate software, that is used to hack into the victim's computer. (2)

V

Vulnerability A weakness, or exposure of an application, system, device, or service that could allow a threat source to breach confidentiality, integrity, or availability.

Sources

(1) "Committee on National Security Systems (CNSS) Glossary." CNSSI No. 4009. Committee on National Security Systems, 2015. Web. Accessed Feb. 2020.

(2) "NCSC Glossary." National Cyber Security Centre, 2016. Web. Accessed Feb. 2020.

(3) *Merriam-Webster.com Dictionary*, Merriam-Webster. Accessed Feb. 2020.

(4) NIST Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary. Accessed Mar. 2020

(5) Wikipedia, https://en.wikipedia.org/wiki. Accessed Mar. 2020.