Rangeview High School

PROJECT LEAD THE WAY

PLTW

Cybersecurity Course Request

Rangeview High School

Randy Mills

Proposal For Cybersecurity Course

Background

With the explosion of devices in our schools it is important to develop a cadre of people to help make the technology enhance not impede lives. At Rangeview we have a CyberPatriot program that is one of the strongest in the country and one of the largest. We have students doing these kinds of tasks every week as they prepare for competition. These students have gone on to become paid interns at Northrop Grumman and working for other Defense Department contractors developing software and working on machines. The target group for this is any level student who has already shown skills that are at a high level. Our additional goal is for students to be able to leave here with the ability to pass industry assessments and certifications. The hope is to even develop that opportunity in connection with other testing agencies to make these industry tests a part of the process.

The planning for this has been two years in preparation. Randy Mills and his students served as a Alpha testing group to help prepare PLTW to roll out this course nationwide. We have had consultations with District level people from Ed Tech and at the highest level of that department they have been supportive. We have worked with the IT Department as we have introduced Cybersecurity into Rangeview. Our counselors and Department Liaisons have all been supportive and offered ideas and suggestions. Currently the primary instructor would be Randy Mills who is currently the Technology Coordinator for Rangeview. Randy has his CTE certification in Information Technology and Business and is a PLTW Master Teacher for the Cybersecurity class. This is an opportunity to be a leader in Computer Science in APS, Colorado, and the United States.

PLTW | Computer Science

Cybersecurity (SEC) High School Course

Executive Summary

Purpose: Cybersecurity (SEC) will be the second course in the Computer Science high school pathway and will introduce students to the many aspects of information security. As this course will require background in computational thinking and basic coding, Introduction to Computer Science (ICS), the first course in the pathway, will be recommended as a pre-requisite

Goals*:* The goals of Cybersecurity will align with the recently established PLTW institutional goals.

1. Provide an inspiring and empowering student experience.
2. Encourage expanded access of the program to ever-increasing numbers of diverse students.
3. Transform teaching practice.
4. Support a thriving enterprise.

General Course Content: The course will be designed to expose high school students to the ever-growing and far-reaching field of cybersecurity. This may be accomplished through problem-based learning where students role-play cybersecurity experts-in-training. The course intends to cover a wide breadth of content related to information security and will promote ethical behavior, technical expertise, professionalism, and communication skills.

Proposed Course Concepts

- *Ethics*: Evaluate ethical impact of cybersecurity situations and the short- and long-term consequences
- *Security:* Conceptualize, design and build secure information technology (IT) systems
- *Protection*: Identify and analyze threats to computer systems and networks
- *Defense:* Establish protective measures to defend secure information
- *Operations*: Administer and monitor IT systems to ensure performance and security are appropriately balanced
- *Analysis*: Collect, review and evaluate cybersecurity information to determine its usefulness
- *Investigation*: Investigate cyber events and crimes against IT systems, networks, and digital information
- *Careers*: Research the many careers and fields that include information security

Educational Standards Alignment

Standards for cybersecurity have evolved over the past decade. A large scale governing framework has been finalized by the National Institute of Standards and Technology (NIST) through the National Initiative for Cybersecurity Education (NICE). The standards are documented in the National Cybersecurity Workforce Framework (also known as the NICE Framework or NCWF), and were developed by numerous academic, industry, and government organizations. The NCWF objectives address topics that span K-12 education and can guide learning progressions.

The content of SEC will align with many of knowledge, skills and abilities set forth in the NICE Framework. It will incorporate many of the big ideas and learning objectives outlined by the College Board and addressed in CSP and CSA. It will also incorporate Computer Science Teachers Association (CSTA) standards and International Society for Technology Education (ISTE) standards as they relate to information security and digital citizenship. Finally, the course will address Common Core State Standards for Literacy in Science & Technical Subjects and select Writing, Speaking and Listening Standards for grade 10.

Tools, Technology and Curriculum

The tools used in the course are numerous and ever-changing. They include

- system administration tools
- network analysis tools
- modeling and data visualization applications
- web-based cybersecurity competitions and capture the flag games

Students will learn the command line interface to the UNIX and DOS operating systems to access most of the tools, which are built-in to the operating system. Occasionally, students will use trusted, open-source software that is freely available on the web.

While learning these tools in the classroom, students will explore and test their cybersecurity skills using a Virtual Private Network (VPN). The VPN will be removed and isolated from any "real" or "live" network and will provide physical and logical boundaries in which the students will work. This will prohibit them from using their new-found skills on other systems and eliminates potential harm (intentional or unintentional) to real data. Outside of the classroom however, students may choose to apply their skills in a negative or harmful manner. For this reason, ethics and altruistic behavior will be a strong focus throughout the course. More on this topic is discussed in the "Special Considerations" section below.

A major focus of the course will be to inspire students to consider a future education and career in cybersecurity. Government and industry are eager to expand the cybersecurity workforce of our nation. The Department of Homeland Security partners with the National Initiative for Cybersecurity Careers and Studies (NICCS) to serve as a national resource for exploring cybersecurity education and career opportunities. Students will make use of this service to learn about accredited cybersecurity schools and the wide breadth of cybersecurity careers.

Instructional Design

While preceding PLTW courses introduce cyber-hygiene, cyber-ethics and basic cybersecurity, this year long course will expand problem solving and computational thinking techniques to demystify how computer systems are structured and organized and how they communicate. In a field that can seem rather daunting, course will be designed to increase accessibility and build confidence in a field that may seem rather daunting to many students. One approach is to have students follow a series of scenarios that simulate real-world cybersecurity situations. Each scenarios will be presented as a small mystery story, or vignette, where students explore security issues and learn a wide range of cybersecurity concepts. At the end of the course, students will use digital forensics tools to find the guilty parties in each of the preceding vignettes.

The goal of the vignette approach is to reduce anxiety over rigorous content, incrementally build skills through engaging real-world scenarios, and provide personal investment in the consequences of decisions in a cyber world. As each vignette will focus on a different contextual application of cybersecurity, they can draw students from a wide variety of backgrounds and experiences and allow students to explore a variety of roles related to information security. As philosophers and social scientists, students can weigh the consequences and societal impact of cybersecurity misconduct. Technical specialists can master operating system skills. Detectives can identify cyber crimes, including malware attacks, corporate security breaches, and identity theft. Finally, acting as legal experts, students can investigate and build a case against those responsible for malicious attacks. In each role, students will explore the ethical impact of the situations they face, the ethical value of their choices, and the consequences of their actions on their future. They will make meaningful connections about the lasting impact of their actions and decisions. Specifically, students should have the opportunity to

- explore ethics to establish "good" and "bad" cyber habits
- use system defense technologies to protect information
- witness breaches, viruses, phishing and other black-hat attacks
- perform cyber forensics to discover criminal behavior
- examine the legality of behavior

Students will acquire a variety of skills and knowledge throughout their role-playing experience and will apply them to problems they might face in cyberspace. Examples of skills and problems to which they can be applied may include

Activities and Projects	*Problem*

Learn the tools available for evaluating and securing information systems	Design a security plan for the system
Learn how to analyze network traffic	Analyze real-time traffic and detect a variety "live" threats
Assess the risks and vulnerabilities of a system	Recognize the consequences of a breach and restore security.
Learn investigative tools and the legal system around cybersecurity	Identify criminals and create a legal case against them

Students will work in teams and paired programming groups, collaborating on all aspects of cybersecurity. The course will allow ample opportunities for collaboration, competition, discovery, invention, game-playing, and other broadly appealing learning paradigms. With the relevant, real-world storylines, students will have an engaging context in which to acquire the rigorous content.

Special Considerations: In addition to the engaging curriculum, cybersecurity is a sensitive issue regarding the ethical use of students acquired skills. Throughout the curriculum, every effort will be made to present the skills and knowledge in a trustworthy and beneficial manner. While all students will be encouraged to make responsible decisions, some students may try to use their knowledge in a harmful manner. While this ethical choice is present for all computer sciences courses, it is of special concern for cybersecurity. Care and consideration will go into designing a course experience where students learn ethical limits as well as the consequences for stepping outside of those limits. The ethical and responsible use of cybersecurity knowledge will be woven throughout the course and will be emphasized as students acquire new skills. Extensive professional development will be built in to assure that teachers are comfortable maintaining these limits and establishing consequences.

The Result

The PLTW Cybersecurity course will provide students a broad exposure to the many aspects of digital and information security while encouraging socially responsible choices and ethical behavior. It will inspire algorithmic thinking and computational thinking, especially "outside the box" thinking skills. It will expose students to the many educational and career paths available to cybersecurity experts as well as other careers that comprise information security.

References

National Cybersecurity Workforce Framework. (2016). https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

[Interim] CSTA K-12 Computer Science Standards. (2016). https://c.ymcdn.com/sites/www.csteachers.org/resource/resmgr/Docs/Standards/2016StandardsRevision/INTERIM_StandardsFINAL_07222.pdf

PLTW Computer Science
Cybersecurity | Course Outline

Identify cybersecurity threats and protect against them. Detect intrusions and respond to attacks. Begin to examine your own digital footprint and better defend your own personal data. Learn how organizations protect themselves in todays world.

Whether seeking a career in the emerging field of cybersecurity or learning to defend your own personal data or a companies. Data students in PLTW Cybersecurity will establish an ethical code of conduct while learning to defend data in today's complex cyber-world.

PLTW Cybersecurity is designed to be a full year (180-day) course for implemented in 10th grade or above. The course is designed to expose high school students to the ever-growing and far-reaching field of cybersecurity. This will be accomplished through problem-based learning where students role-play as cybersecurity experts and train as cybersecurity expert do.

PLTW Cybersecurity is designed with strong connections to the National Cybersecurity Workforce Framework (also known as the NICE Framework or NCWF). This framework created by the National Institute of Standards and Technology (NIST) identifies standards that have been developed by numerous academic, industry, and government organizations and the objectives address topics that span K-12 education and guide learning progressions.

The course also incorporates many of the big ideas and learning objectives outlined by the College Board and addressed in AP CSP and AP CSA as well as incorporating Computer Science Teachers Association (CSTA) standards and International Society for Technology Education (ISTE) standards as they relate to information security and digital citizenship.

PLTW Cybersecurity will provide students a broad exposure to the many aspects of digital and information security while encouraging socially responsible choices and ethical behavior. It will inspire algorithmic thinking, computational thinking, and especially "outside the box" thinking. Students will explore the many educational and career paths available to cybersecurity experts as well as other careers that comprise information security. The following is a list of the units of study in the course.

Unit 1	Personal Cybersecurity
Unit 2	System Cybersecurity
Unit 3	Enterprise Cybersecurity
Unit 4	Applied Cybersecurity: Digital Forensics

Unit 1: Personal Cybersecurity

Students will learn the basic concepts of cybersecurity by leveraging their familiarity with technology they use every day, such as mobile devise and apps, email and personal files, and social networking habits.

Personal Cybersecurity

Lesson 1.1	Introduction to Cybersecurity
Lesson 1.2	On the Internet
Lesson 1.3	Protect Your Data

Lesson 1.1: Personal Security

Students will learn personal and digital security, describe why it is important, and learn to be safe consumers of digital information in a variety of contexts.

Activity 1.1.1	Codes of Conduct
Activity 1.1.2	Password Protection and Authentication
Activity 1.1.3	Email and Social Media Security Risks
Project 1.1.4	Ethical Hacking: Save the Day

Lesson 1.2: The Internet Security

Students will learn that the internet is a loosely controlled collection of computers that are networked together. They will learn about firewalls and their role in a network. They will learn basic types of malware, safe browsing habits, and security features of their browser. At the end of the lesson, students will discover that they are the victim of a browser attack. They will determine how the attack occurred, manage the security of the firewall, and secure their browser.

Activity 1.2.1	Firewalls and Malware
Activity 1.2.2	Spotting Browser Attacks
Project 1.2.3	It’s a Trap!

Lesson 1.3: Getting to Know Your Data: Recover and Protect

Students will learn that all data residing on a computer are actually files. They will learn various ways to manage, store, and secure data. They will learn about user and system processes, how to manage them, and how to identify suspicious processes (potential malware). Finally they will use their knowledge about files, directories, processes, browsers, suspicious emails and malware to solve the unit problem.

Activity 1.3.1:	Files and Processes
Problem 1.3.2:	A Dangerous Absence

Unit 2: System Security

Students will broaden their cybersecurity knowledge from a personal level to a larger networked system. They will explore local area networks, the UNIX operating system and how to assess the value of information security.

System Security

Lesson 2.1:	The Value of Information

Lesson 2.2:	UNIX, the Internet's Operating System
Lesson 2.3:	Networks in Depth
Lesson 2.4:	The Hacked Hospital

Lesson 2.1: The Value of Information

Students will dive deeper into information confidentiality and how it relates to its integrity and assurance. They will compare the value and the risks of sharing information, how to define a local area network, explore the security a small network, and identify a variety of physical security measures.

Activity 2.1.1 Confidentiality, Integrity, and Availability
Activity 2.1.2 LAN Architecture
Project 2.1.3 Protect the Patient

Lesson 2.2: UNIX, the Internet's Operating System

Students will learn more about the types of malware that are threats to information and their delivery systems. They will use UNIX commands and configuration tools to secure digital information.

Activity 2.2.1 More on Malware
Activity 2.2.2 UNIX Uncovered
Project 2.2.3 Find the Secret Message

Lesson 2.3: Networks in Depth

Students will learn about UNIX processes and how malware spreads around a network. They will learn how to control access to information by controlling file access, manage groups, and setting privileges.

Activity 2.3.1 Processes, Processes, and more Processes
Activity 2.3.2 How Does Malware Spread?
Activity 2.3.3 User Privileges
Project 2.3.4 Rogue N

Lesson 2.4: The Hacked Hospital

The focus of this lesson is the end of unit problem in which students discover a breach, find the files that were affected, manage processes that were responsible, establish user and group access to digital and physical assets, and then add design elements to the network to secure it.

Activity 2.4.1: Where Can I Learn More about Cybersecurity?
Problem 2.4.2: Helping Cyber Hospital

Unit 3: Enterprise Cybersecurity

Students will learn the technical aspects of a highly networked world, and the risks to the information we all share. They will learn networking concepts such as subnets, dynamic host configuration, packet analysis, and virtual networks. They will learn the types of malware that can attack systems on a network and how to secure and protect a system against them.

Enterprise Cybersecurity	
Lesson 3.1:	Clouds and Other Nebulous Things
Lesson 3.2:	Attacks from the Net
Lesson 3.3:	Analyzing the Net

Lesson 3.1: Clouds and Other Nebulous Things

Students will demystify the "cloud" and learn how networks can grow to a large size. Then, they learn how to define a virtual local area network (LAN) and how to secure systems on a network. Finally they will search a network to discover a host that has low or vulnerable security.

Activity 3.1.1	What Exactly is the Cloud?
Activity 3.1.2	The Edge of the Network
Project 3.1.3	Find the Vulnerable Host

Lesson 3.2: Attacks from the Net

Students learn how host names are related to digital addresses and the layered, abstracted nature of data transfer on the Internet. They further explore network topologies and go deeper down the abstraction path to learn about network security. Finally, the will explore a network of systems to find an exploit on one, vulnerable system.

Activity 3.2.1	Network Information, Organized!
Activity 3.2.2	Exploring Network Security
Project 3.2.4	Find the Exploits

Lesson 3.3: Analyzing the Net

The focus of Lesson 3 will be analyzing network traffic to witness and then protect against a malware attack. They will analyze packets to find telltale signs and patterns of malicious exploits. They will apply what they've learned to perform a penetration test and to secure a network against further attacks.

Activity 3.3.1	Packets
Activity 3.3.2	Attack Analysis
Project 3.3.3	Pen Test: Red Team, Blue Team

Lesson 3.4 Infrastructure Incident

Students will be presented with a scenario in which a water treatment facility has been hacked. They will identify how the breach occurred, fix the problems the breach may have caused, and modify the system to prevent future attacks

Problem 3.3.4 Restore the Infrastructure

Unit 4: Applied Cybersecurity: Digital Forensics

Students will explore cybersecurity in an applied field; digital forensics. They will gain a broad understanding of the forensics process and explore methods of cryptography and steganography. They will "process" a crime scene to solve the mystery, and explore the possible consequences of the crime.

Applied Cybersecurity: Digital Forensics

Lesson 4.1: Data as Evidence
Lesson 4.2: Solving Cybercrimes
Lesson 4.3: The Crime Scene

Lesson 4.1: Data as Evidence

Students learn about digital forensics and why it is important. They will explore cybercrime and how to define it. Students will learn the history of encryption and ciphers and use frequency predictors to try to break codes. Finally, they will practice data hiding techniques such as cryptography and steganography.

Activity 4.1.1 Ciphers and Cryptography
Activity 4.1.2 Uses of Encryption
Project 4.1.3 Decrypt the Encrypted

Lesson 4.2: Solving Cybercrimes

Students learn the process of gathering digital evidence, analyzing it, tracing the criminal through their digital footprint, and preparing to prosecute the criminal.

Activity 4.2.1: Tools of the Trade
Activity 4.2.2: Tracing Identity
Activity 4.2.3: Preparing a Rock-Solid Case
Project 4.2.4: Make Your Discovery

Lesson 4.3: The Crime Scene

Students use all of their skills to identify the crime(s) committed, collect evidence, secure data, analyze data, assess damage, follow a digital footprint, identify the criminals, and bring them to justice.

Problem 4.3.1: Solve the Crime!

Cybersecurity - CSTA K-12 Computer Science Standards Level 3A: Grades 9-10

Unit 1

Lessons						
1-1	**1-2**	**1-3**	Identifer			
		x	3A-IC-27	Impacts of Computing	Social Interactions	Use tools and methods for collaboration on a project to increase connectivity of people in different cultures and career fields.
		x	3A-AP-23	Algorithms and Programming	Program Development	Document design decisions using text, graphics, presentations, and/or demonstrations in the development of complex programs.
		x	3A-AP-22	Algorithms and Programming	Program Development	Design and develop computational artifacts working in team roles using collaborative tools.
		x	3A-DA-11	Data and Analysis	Collection Visualization & Transformation	Create interactive data visualizations using software tools to help others better understand real-world phenomena.
	x		3A-NI-08	Networks and the Internet	Cybersecurity	Explain tradeoffs when selecting and implementing cybersecurity recommendations.
	x		3A-NI-07	Networks and the Internet	Network Communication & Organization	Compare various security measures, considering tradeoffs between the usability and security of a computing system.
	x	x	3A-DA-10	Data and Analysis	Storage	Evaluate the tradeoffs in how data elements are organized and where data is stored.
	x	x	3A-NI-04	Networks and the Internet	Network Communicotion & Organization	Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing
x	x	x	3A-IC-24	Impacts of Computing	Culture	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
x	x	x	3A-NI-06	Networks and the Internet	Cybersecurity	Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.
x	x	x	3A-NI-05	Networks and the Internet	Network Communication & Organization	Give examples to illustrate how sensitive data can be affected by malware and other attacks.

Cybersecurity - CSTA K-12 Computer Science Standards Level 3A: Grades 9-10

Unit 2

Lessons						
2-1	**2-2**	**2-3**	**2-4**	Identifier		
			x	3A-IC-27	Impacts of Computing	Social Interactions
				Use tools and methods for collaboration on a project to increase connectivity of people in different cultures and career fields.		
x	x	x	x	3A-IC-24	Impacts of Computing	Culture
				Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.		
		x		3A-AP-23	Algorithms and Programming	Program Development
				Document design decisions using text, graphics, presentations, and/or demonstrations in the development of complex programs.		
		x		3A-AP-22	Algorithms and Programming	Program Development
				Design and develop computational artifacts working in team roles using collaborative tools.		
x		x		3A-DA-12	Data and Analysis	Inference & Models
				Create computational models that represent the relationships among different elements of data collected from a phenomenon or process.		
			x	3A-DA-11	Data and Analysis	Collection Visualization & Transformation
				Create interactive data visualizations using software tools to help others better understand real-world phenomena.		
		x	x	3A-DA-10	Data and Analysis	Storage
				Evaluate the tradeoffs in how data elements are organized and where data is stored.		
x			x	3A-NI-08	Networks and the Internet	Cybersecurity
				Explain tradeoffs when selecting and implementing cybersecurity recommendations.		
x			x	3A-NI-07	Networks and the Internet	Network Communication & Organization
				Compare various security measures, considering tradeoffs between the usability and security of a computing system.		
x	x	x	x	3A-NI-06	Networks and the Internet	Cybersecurity
				Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.		
x	x	x	x	3A-NI-05	Networks and the Internet	Network Communication & Organization
				Give examples to illustrate how sensitive data can be affected by malware and other attacks.		

Lessons						
2-1	**2-2**	**2-3**	**2-4**	Identifier		
x		x	x	3A-NI-04	Networks and the Internet	Network Communicotion & Organization
				Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing		
x	x		x	3A-CS-02	Computing Systems	Hardware & Software
				Compare levels of abstraction and interactions between application software, system software, and hardware layers.		

Cybersecurity - CSTA K-12 Computer Science Standards Level 3B: 11-12

Unit 2

Lessons							
2-1	**2-2**	**2-3**	**2-4**	Identifier			
	x			3B-IC-28	Impacts of Computing	Safety Law and Ethics	Debate laws and regulations that impact the development and use of software.
			x	3B-IC-25	Impacts of Computing	Culture	Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society.
	x			3B-AP-22	Algorithms and Programming	Program Development	Modify an existing program to add additional functionality and discuss intended and unintended implications (e.g., breaking other functionality).
	x			3B-AP-18	Algorithms and Programming	Program Development	Explain security issues that might lead to compromised computer programs.
		x	x	3B-DA-05	Data and Analysis	Collection Visualization and Transformation	Use data analysis tools and techniques to identify patterns in data representing complex systems.
x				3B-NI-04	Networks and the Internet	Cybersecurity	Compare ways software developers protect devices and information from unauthorized access.
x	x	x	x	3B-NI-03	Networks and the Internet	Network Communication and Orhganization	Describe the issues that impact network functionality (e.g., bandwidth, load, delay, topology).
			x	3B-CS-02	Computing Systems	Troubleshooting	Illustrate ways computing systems implement logic, input, and output through hardware components.
	x	x	x	3B-CS-01	Computing Systems	Hardware & Software	Categorize the roles of operating system software.
	x	x	x	3B-CS-01	Computing Systems	Hardware & Software	Categorize the roles of operating system software.

PROJECT LEAD THE WAY PLTW

Cybersecurity - CSTA K-12 Computer Science Standards Level 3A: Grades 9-10

Unit 3

Lessons							
3-1	3-2	3-3	3-4	Identifer			
			x	3A-IC-27	Impacts of Computing	Social Interactions	Use tools and methods for collaboration on a project to increase connectivity of people in different cultures and career fields.
x	x	x	x	3A-IC-24	Impacts of Computing	Culture	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
		x	x	3A-AP-23	Algorithms and Programming	Program Development	Document design decisions using text, graphics, presentations, and/or demonstrations in the development of complex programs.
			x	3A-AP-22	Algorithms and Programming	Program Development	Design and develop computational artifacts working in team roles using collaborative tools.
x	x	x	x	3A-AP-21	Algorithms and Programming	Program Development	Evaluate and refine computational artifacts to make them more usable and accessible.
x	x		x	3A-DA-12	Data and Analysis	Inference & Models	Create computational models that represent the relationships among different elements of data collected from a phenomenon or process.
			x	3A-DA-11	Data and Analysis	Collection Visualization & Transformation	Create interactive data visualizations using software tools to help others better understand real-world phenomena.
x	x	x	x	3A-DA-10	Data and Analysis	Storage	Evaluate the tradeoffs in how data elements are organized and where data is stored.
			x	3A-NI-08	Networks and the Internet	Cybersecurity	Explain tradeoffs when selecting and implementing cybersecurity recommendations.
			x	3A-NI-07	Networks and the Internet	Network Communication & Organization	Compare various security measures, considering tradeoffs between the usability and security of a computing system.
x	x	x	x	3A-NI-06	Networks and the Internet	Cybersecurity	Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

Lessons

3-1	3-2	3-3	3-4	Identifer		
x	x	x	x	3A-NI-05	Networks and the Internet	Network Communication & Organization
				Give examples to illustrate how sensitive data can be affected by malware and other attacks.		
x	x	x	x	3A-NI-04	Networks and the Internet	Network Communicotion & Organization
				Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing		
x	x	x	x	3A-CS-02	Computing Systems	Hardware & Software
				Compare levels of abstraction and interactions between application software, system□oftware, and hardware layers.		

Cybersecurity - CSTA K-12 Computer Science Standards Level 3B: 11-12

Unit 3

Lessons							
3-1	3-2	3-3	3-4	Identifer			
		x		3B-IC-28	Impacts of Computing	Safety Law and Ethics	Debate laws and regulations that impact the development and use of software.
x	x	x		3B-IC-25	Impacts of Computing	Culture	Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society.
			x	3B-AP-22	Algorithms and Programming	Program Development	Modify an existing program to add additional functionality and discuss intended and unintended implications (e.g., breaking other functionality).
			x	3B-AP-18	Algorithms and Programming	Program Development	Explain security issues that might lead to compromised computer programs.
	x	x		3B-AP-15	Algorithms and Programming	Modularity	Analyze a large-scale computational problem and identify generalizable patterns that can be applied to a solution.
			x	3B-AP-10	Algorithms and Programming	Algorithms	Use and adapt classic algorithms to solve computational problems.
		x		3B-DA-06	Data and Analysis	Collection Visualization and Transformation	Select data collection tools and techniques to generate data sets that support a claim or communicate information.
x	x	x	x	3B-DA-05	Data and Analysis	Collection Visualization and Transformation	Use data analysis tools and techniques to identify patterns in data representing complex systems.
			x	3B-NI-04	Networks and the Internet	Cybersecurity	Compare ways software developers protect devices and information from unauthorized access.
x	x	x		3B-NI-03	Networks and the Internet	Network Communication and Orhganization	Describe the issues that impact network functionality (e.g., bandwidth, load, delay, topology).
x	x	x		3B-CS-02	Computing Systems	Troubleshooting	Illustrate ways computing systems implement logic, input, and output through hardware components.

Lessons						
3-1	**3-2**	**3-3**	**3-4**	Identifer		
x	x	x		3B-CS-01	Computing Systems	Hardware & Software
				Categorize the roles of operating system software.		
x	x	x		3B-CS-01	Computing Systems	Hardware & Software
				Categorize the roles of operating system software.		

PROJECT LEAD THE WAY PLTW

Cybersecurity - CSTA K-12 Computer Science Standards Level 3A: Grades 9-10

Unit 4

Lessons						
4-1	**4-2**	**4-3**	Identifer			
		x	3A-DA-12	Data and Analysis	Inference & Models	Create computational models that represent the relationships among different elements of data collected from a phenomenon or process.
		x	3A-NI-04	Networks and the Internet	Network Communicotion & Organization	Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing
x	x	x	3A-NI-05	Networks and the Internet	Network Communication & Organization	Give examples to illustrate how sensitive data can be affected by malware and other attacks.
x	x	x	3A-NI-06	Networks and the Internet	Cybersecurity	Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.
		x	3A-NI-07	Networks and the Internet	Network Communication & Organization	Compare various security measures, considering tradeoffs between the usability and security of a computing system.
		x	3A-NI-08	Networks and the Internet	Cybersecurity	Explain tradeoffs when selecting and implementing cybersecurity recommendations.
x			3A-DA-09	Data and Analysis	Storage	Translate between different bit representations of real-world phenomena, such as characters, numbers, and images.
x		x	3A-CS-02	Computing Systems	Hardware & Software	Compare levels of abstraction and interactions between application software, system software, and hardware layers.
		x	3A-DA-11	Data and Analysis	Collection Visualization & Transformation	Create interactive data visualizations using software tools to help others better understand real-world phenomena.
		x	3A-IC-27	Impacts of Computing	Social Interactions	Use tools and methods for collaboration on a project to increase connectivity of people in different cultures and career fields.
x			3A-AP-13	Algorithms and Programming	Algorithms	Create prototypes that use algorithms to solve computational problems by leveraging prior student knowledge and personal interests.

Lessons					
4-1	**4-2**	**4-3**	Identifer		
x			3A-AP-14	Algorithms and Programming	Variables
			Use lists to simplify solutions, generalizing computational problems instead of repeatedly using simple variables.		
x		x	3A-AP-21	Algorithms and Programming	Program Development
			Evaluate and refine computational artifacts to make them more usable and accessible.		
		x	3A-AP-22	Algorithms and Programming	Program Development
			Design and develop computational artifacts working in team roles using collaborative tools.		
		x	3A-AP-23	Algorithms and Programming	Program Development
			Document design decisions using text, graphics, presentations, and/or demonstrations in the development of complex programs.		
x	x	x	3A-IC-24	Impacts of Computing	Culture
			Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.		
x			3A-IC-26	Impacts of Computing	Culture
			Demonstrate ways a given algorithm applies to problems across disciplines.		
		x	3A-DA-10	Data and Analysis	Storage
			Evaluate the tradeoffs in how data elements are organized and where data is stored.		

Cybersecurity - CSTA K-12 Computer Science Standards Level 3B: 11-12

Unit 4

Lessons						
4-1	4-2	4-3	Identifer			
x	x		3B-IC-28	Impacts of Computing	Safety Law and Ethics	Debate laws and regulations that impact the development and use of software.
x	x		3B-IC-25	Impacts of Computing	Culture	Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society.
	x		3B-AP-15	Algorithms and Programming	Modularity	Analyze a large-scale computational problem and identify generalizable patterns that can be applied to a solution.
x	x		3B-DA-06	Data and Analysis	Collection Visualization and Transformation	Select data collection tools and techniques to generate data sets that support a claim or communicate information.
x	x		3B-DA-05	Data and Analysis	Collection Visualization and Transformation	Use data analysis tools and techniques to identify patterns in data representing complex systems.
	x		3B-NI-03	Networks and the Internet	Network Communication and Orhganization	Describe the issues that impact network functionality (e.g., bandwidth, load, delay, topology).
	x		3B-CS-02	Computing Systems	Troubleshooting	Illustrate ways computing systems implement logic, input, and output through hardware components.
	x		3B-CS-01	Computing Systems	Hardware & Software	Categorize the roles of operating system software.
	x		3B-CS-01	Computing Systems	Hardware & Software	Categorize the roles of operating system software.

Cybersecurity - National Initiative for Cybersecurity Education

Unit 1

Lessons			
1-1	**1-2**	**1-3**	Identifer
		x	A0062 Monitor measures or indicators of system performance and availability.
		x	A0013 Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
		x	A0019 Produce technical documentation.
		x	A0021 Use and understand complex mathematical concepts (e.g., discrete math, boolean algebra)
		x	A0120 Share meaningful insights about the context of an organization’s threat environment that improve its risk management posture.
		x	A0105 Tailor technical and planning information to a customer’s level of understanding.
	x		A0026 Analyze test data
	x		A0001 Identify systemic security issues based on the analysis of vulnerability and configuration data.
	x	x	A0025 Accurately define incidents, problems, and events
	x	x	A0040 Translate data and test results into evaluative conclusions
	x	x	A0070 Ability to apply critical reading/thinking skills.

Lessons			
1-1	**1-2**	**1-3**	Identifer
x			K0158 Know organizational information technology (it) user security policies (e.g., account creation, password rules, access control).
x			S0052 Use social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).
x		x	A0085 Exercise judgment when policies are not well-defined.
x		x	A0092 Identify/describe target vulnerability.
x	x		A0042 Develop career path opportunities
x	x	x	A0074 Collaborate effectively with others.
x	x	x	A0106 Ability to think critically.
x	x	x	A0123 Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
x	x	x	A0155 Provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities.
x	x	x	A0014 Communicate effectively when writing.
x	x	x	A0069 Ability to apply collaborative skills and strategies.

Cybersecurity - National Initiative for Cybersecurity Education

Unit 2

Lessons				
2-1	**2-2**	**2-3**	**2-4**	Identifier
			x	A0025 Accurately define incidents, problems, and events
		x		A0055 Operate common network tools (e.g., ping, traceroute, nslookup).
x		x	x	A0049 Apply secure system design tools, methods and techniques.
		x	x	A0048 Apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
		x	x	A0042 Develop career path opportunities
		x		A0041 Use data visualization tools
			x	A0040 Translate data and test results into evaluative conclusions
		x	x	A0035 Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.
x		x	x	A0030 Collect, verify, and validate test data
		x	x	A0001 Identify systemic security issues based on the analysis of vulnerability and configuration data.
		x	x	A0026 Analyze test data

Lessons				
2-1	**2-2**	**2-3**	**2-4**	Identifier
	x		x	A0062 Monitor measures or indicators of system performance and availability.
			x	A0019 Produce technical documentation.
		x	x	A0015 Conduct vulnerability scans and recognize vulnerabilities in security systems.
			x	A0014 Communicate effectively when writing.
			x	A0013 Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
			x	A0012 Ask clarifying questions
			x	A0011 Answer questions in a clear and concise manner.
	x	x	x	A0010 Analyze malware.
		x	x	A0003 Determine the validity of technology trend data.
			x	A0027 Apply an organization's goals and objectives to develop and maintain architecture
x	x		x	A0093 Identify/describe techniques/methods for conducting technical exploitation of the□target.
x			x	A0155 Provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities.
		x	x	A0128 Apply techniques for detecting host and network-based intrusions using intrusion□detection technologies.

Lessons				
2-1	**2-2**	**2-3**	**2-4**	Identifier
		x		A0126 Ability to track the location and configuration of networked devices and software across departments, locations, facilities and, potentially, supporting business functions.
x			x	A0123 Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
x			x	A0120 Share meaningful insights about the context of an organization’s threat environment that improve its risk management posture.
x	x	x	x	A0107 Think like threat actors.
x	x	x	x	A0106 Ability to think critically.
			x	A0105 Tailor technical and planning information to a customer’s level of understanding.
		x		A0058 Execute os command line (e.g., ipconfig, netstat, dir, nbtstat).
			x	A0097 Ability to monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity.
x				A0061 Design architectures and frameworks.
			x	A0092 Identify/describe target vulnerability.
			x	A0086 Expand network access by conducting target analysis and collection to identify targets of interest.
			x	A0085 Exercise judgment when policies are not well-defined.
x	x	x	x	A0083 Evaluate information for reliability, validity, and relevance.

Lessons				
2-1	**2-2**	**2-3**	**2-4**	Identifier
			x	A0074 Collaborate effectively with others.
			x	A0070 Ability to apply critical reading/thinking skills.
			x	A0069 Ability to apply collaborative skills and strategies.
			x	A0067 Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.
			x	A0172 Set up a physical or logical sub-networks that separates an internal local area network (lan) from other untrusted networks.
	x		x	A0101 Recognize and mitigate cognitive biases which may affect analysis.

Cybersecurity - National Initiative for Cybersecurity Education

Unit 3

Lessons				
3-1	**3-2**	**3-3**	**3-4**	Identifer
	x	x		A0026 Analyze test data
		x	x	A0062 Monitor measures or indicators of system performance and availability.
		x	x	A0061 Design architectures and frameworks.
x	x	x	x	A0059 Operate the organization's lan/wan pathways.
x	x	x	x	A0058 Execute os command line (e.g., ipconfig, netstat, dir, nbtstat).
x	x	x	x	A0055 Operate common network tools (e.g., ping, traceroute, nslookup).
x	x	x	x	A0052 Operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
x	x	x	x	A0049 Apply secure system design tools, methods and techniques.
x	x	x	x	A0048 Apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
			x	A0041 Use data visualization tools
	x	x		A0040 Translate data and test results into evaluative conclusions

Lessons				
3-1	**3-2**	**3-3**	**3-4**	Identifer
x	x	x	x	A0001 Identify systemic security issues based on the analysis of vulnerability and configuration data.
	x	x		A0030 Collect, verify, and validate test data
			x	A0069 Ability to apply collaborative skills and strategies.
	x			A0025 Accurately define incidents, problems, and events
		x	x	A0021 Use and understand complex mathematical concepts (e.g., discrete math, boolean algebra)
	x	x	x	A0019 Produce technical documentation.
x	x	x	x	A0015 Conduct vulnerability scans and recognize vulnerabilities in security systems.
			x	A0014 Communicate effectively when writing.
			x	A0013 Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
			x	A0012 Ask clarifying questions
			x	A0011 Answer questions in a clear and concise manner.
x	x	x	x	A0010 Analyze malware.
		x	x	A0003 Determine the validity of technology trend data.

Lessons				
3-1	**3-2**	**3-3**	**3-4**	Identifer
	x		x	A0035 Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.
x	x	x	x	A0097 Ability to monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity.
	x			A0172 Set up a physical or logical sub-networks that separates an internal local area network (lan) from other untrusted networks.
x	x	x	x	A0159 Interpret the information collected by network tools (e.g. nslookup, ping, and traceroute).
		x	x	A0155 Provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities.
x	x	x	x	A0128 Apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
x	x	x	x	A0127 Ability to deploy continuous monitoring technologies and tools.
		x	x	A0126 Ability to track the location and configuration of networked devices and software across departments, locations, facilities and, potentially, supporting business functions.
	x	x	x	A0124 Establish and maintain automated security control assessments
			x	A0113 Determine whether a security incident violates a privacy principle or legal standard requiring specific legal action.
x	x	x	x	A0107 Think like threat actors.
x	x	x	x	A0106 Ability to think critically.
x	x	x	x	A0065 Monitor traffic flows across the network.

Lessons				
3-1	**3-2**	**3-3**	**3-4**	Identifer
		x	x	A0101 Recognize and mitigate cognitive biases which may affect analysis.
			x	A0067 Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.
x		x	x	A0096 Ability to interpret and understand complex and rapidly evolving concepts.
		x	x	A0093 Identify/describe techniques/methods for conducting technical exploitation of the target.
		x	x	A0092 Identify/describe target vulnerability.
		x	x	A0086 Expand network access by conducting target analysis and collection to identify targets of interest.
			x	A0085 Exercise judgment when policies are not well-defined.
x	x	x	x	A0084 Evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.
x	x	x	x	A0083 Evaluate information for reliability, validity, and relevance.
		x	x	A0080 Develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
			x	A0074 Collaborate effectively with others.
			x	A0070 Ability to apply critical reading/thinking skills.
		x	x	K0158 Know organizational information technology (it) user security policies (e.g., account creation, password rules, access control).

Lessons				
3-1	**3-2**	**3-3**	**3-4**	Identifer
			x	A0105 Tailor technical and planning information to a customer’s level of understanding.

Cybersecurity - National Initiative for Cybersecurity Education

Unit 4

Lessons			
4-1	**4-2**	**4-3**	Identifer
		x	A0027 Apply an organization's goals and objectives to develop and maintain architecture
	x	x	A0001 Identify systemic security issues based on the analysis of vulnerability and configuration data.
	x	x	A0062 Monitor measures or indicators of system performance and availability.
		x	A0061 Design architectures and frameworks.
	x	x	A0059 Operate the organization's lan/wan pathways.
	x	x	A0058 Execute os command line (e.g., ipconfig, netstat, dir, nbtstat).
	x	x	A0055 Operate common network tools (e.g., ping, traceroute, nslookup).
	x	x	A0052 Operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
		x	A0049 Apply secure system design tools, methods and techniques.
		x	A0048 Apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
	x	x	A0043 Conduct forensic analyses in and for both windows and unix/linux environments.

Lessons			
4-1	4-2	4-3	Identifer
	x		A0042 Develop career path opportunities
	x	x	A0067 Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.
	x	x	A0035 Ability to dissect a problem and examine the interrelationships between data that may appear unrelated.
	x	x	A0069 Ability to apply collaborative skills and strategies.
		x	A0025 Accurately define incidents, problems, and events
	x	x	A0021 Use and understand complex mathematical concepts (e.g., discrete math, boolean algebra)
		x	A0019 Produce technical documentation.
		x	A0015 Conduct vulnerability scans and recognize vulnerabilities in security systems.
		x	A0014 Communicate effectively when writing.
		x	A0013 Communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
		x	A0012 Ask clarifying questions
		x	A0011 Answer questions in a clear and concise manner.
		x	A0010 Analyze malware.

Lessons			
4-1	**4-2**	**4-3**	Identifer
x		x	A0005 Decrypt digital data collections.
x		x	A0003 Determine the validity of technology trend data.
	x	x	A0041 Use data visualization tools
	x	x	A0101 Recognize and mitigate cognitive biases which may affect analysis.
	x		S0052 Use social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).
	x	x	A0159 Interpret the information collected by network tools (e.g. nslookup, ping, and traceroute).
	x	x	A0155 Provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities.
		x	A0128 Apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
		x	A0127 Ability to deploy continuous monitoring technologies and tools.
	x	x	A0126 Ability to track the location and configuration of networked devices and software across departments, locations, facilities and, potentially, supporting business functions.
		x	A0124 Establish and maintain automated security control assessments
	x		A0123 Apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
	x	x	A0120 Share meaningful insights about the context of an organization’s threat environment that improve its risk management posture.

Lessons			
4-1	**4-2**	**4-3**	Identifer
	x	x	A0113 Determine whether a security incident violates a privacy principle or legal standard requiring specific legal action.
	x	x	A0107 Think like threat actors.
	x	x	A0065 Monitor traffic flows across the network.
		x	A0105 Tailor technical and planning information to a customer’s level of understanding.
	x		K0158 Know organizational information technology (it) user security policies (e.g., account creation, password rules, access control).
		x	A0097 Ability to monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity.
		x	A0096 Ability to interpret and understand complex and rapidly evolving concepts.
	x	x	A0093 Identify/describe techniques/methods for conducting technical exploitation of the target.
	x	x	A0092 Identify/describe target vulnerability.
	x	x	A0086 Expand network access by conducting target analysis and collection to identify targets of interest.
		x	A0085 Exercise judgment when policies are not well-defined.
		x	A0084 Evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.
x	x	x	A0083 Evaluate information for reliability, validity, and relevance.

Lessons			
4-1	**4-2**	**4-3**	Identifer
x		x	A0080 Develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
	x	x	A0074 Collaborate effectively with others.
	x	x	A0070 Ability to apply critical reading/thinking skills.
x	x	x	A0106 Ability to think critically.