Cybersecurity Fundamentals

6302 36 weeks

Table of Contents

Acknowledgments

The components of this framework were developed by the following business panel team members, who met March 17, 2016:

LaTizzia Bragg-Bullock, Potomac Senior High School, Prince William County Public Schools
Nancy Brandon, Colonial Forge High School, Stafford County Public Schools
Ginger Cromer, Burton Center for Arts and Technology, Roanoke County Public Schools

Gail Drake, Battlefield High School, Prince William County Public Schools, and Associate Professor, Northern Virginia Community College
Dr. Chuck Gardner, Director of Curriculum, National Integrated Cyber Education Research Center, Bossier City, Louisiana
Danielle Hennessey, Assistant Director, Center for Cyber Security and the Center for Financial Responsibility, Longwood University, Farmville
Luke Juday, Research Analyst, University of Virginia Weldon Cooper Center for Public Service, Charlottesville
Linda Lavender, The Advanced Technology Center, Virginia Beach City Public Schools
Margaret Leary, Director/Curriculum, National Cyberwatch Center, Largo, Maryland
Sharon McPherson, Colonial Forge High School, Stafford County Public Schools
Michael Miklich, CEO/President, Cybersecurity Education Inc., Vienna, Virginia
Linda Smith, Mountain View High School, Stafford County Public Schools

The following teachers served on the Curriculum Development team, which met October 18-19, 2016:

Brenda Anderson-Diggs, Essex High School, Essex County Public Schools
Nancy Brandon, Colonial Forge High School, Stafford County Public Schools
Darrell Carpenter, Director, Center for Cyber Security, Longwood University, Farmville
Gail Drake, Battlefield High School, Prince William County Public Schools, and Associate Professor, Northern Virginia Community College
Adrian Foster, Surry County High School, Surry County Public Schools
Dr. Chuck Gardner, Director of Curriculum, National Integrated Cyber Education Research Center, Bossier City, Louisiana
Dr. Megan Healy, Assistant Vice Chancellor for Academics, Virginia Community College System
Brian Jones, Franklin County High School, Franklin County Public Schools
Linda Lavender, The Advanced Technology Center, Virginia Beach City Public Schools
Dr. Prem Uppuluri, Associate Professor, Department of Information Technology, Radford University, Radford
Curtis Woodward, Teacher, Washington County Public Schools

Correlations to the Virginia Standards of Learning were reviewed and updated by:

Norma J. Bonney, Kempsville High School, Virginia Beach City Public Schools
Vickie L. Inge, Mathematics Committee Member, Virginia Mathematics and Science Coalition
Anne F. Markwith, New Teacher Mentor, Gloucester County Public Schools
Cathy Nichols-Cocke, PhD, Fairfax High School, Fairfax County Public Schools
Caroline C. Wheeler, M.T., Secondary English

The framework was edited and produced by the CTE Resource Center:

Kevin P. Reilly, Administrative Coordinator

Judith P. Sams, Specialist, Business and Information Technology and Related Clusters
Office of Career, Technical, and Adult Education
Virginia Department of Education

Dr. Tricia S. Jacobs, CTE Coordinator of Curriculum and Instruction
Office of Career, Technical, and Adult Education
Virginia Department of Education

Course Description

Suggested Grade Level: 9 or 10 or 11 or 12

Cybersecurity affects every individual, organization, and nation. This course focuses on the evolving and pervasive technological environment with an emphasis on securing personal, organizational, and national information. Students will be introduced to the principles of cybersecurity, explore emerging technologies, examine threats and protective measures, and investigate the diverse high-skill, high-wage, and high-demand career opportunities in the field of cybersecurity.

Task Essentials Table

Template material omitted: General material used to introduce the task list has been omitted.

For the indicated course(s):

- Tasks/competencies designated by plus icons (⊕) in the left-hand column(s) are essential
- Tasks/competencies designated by empty-circle icons (○) are optional
- Tasks/competencies designated by minus icons (⊖) are omitted
- Tasks marked with an asterisk (*) are sensitive.

Task Number	6302	Tasks/Competencies
Exploring Cybersecurity Fundamentals		
39	⊕	Describe *cybersecurity*.
40	⊕	Define *information assurance*.

41	⊕	Describe the critical factors of information security.	
42	⊕	Explain cybersecurity services as they relate to intrusion prevention capabilities that protect systems against unauthorized access, exploitation, and data exfiltration.	
43	⊕	Define *risk*.	
44	⊕	Identify the concepts of cybersecurity risk management.	
45	⊕	Describe cybersecurity threats to an organization.	
46	⊕	Explain why organizations need to manage risk.	
47	⊕	Discuss national or industry standards/regulations that relate to cybersecurity.	
48	⊕	Describe the cyberattack surface of various organizations.	
49	⊕	Analyze risks affecting critical infrastructure.	
Examining Computer Networks as a Foundational Element of Cybersecurity			
50	⊕	Describe a network.	
51	⊕	Describe a wired/cabled network.	
52	⊕	Describe a wireless network.	
53	○	Compare cabled/wired and wireless networks.	
54	○	Compare networking conceptual models.	
55	○	Discuss services, their relationship to the OSI model, and potential vulnerabilities.	
56	⊕	Differentiate among network types.	
57	⊕	Examine the concept of the Internet as a network of connected systems.	
58	⊕	Identify networking protocols.	
Understanding Cyber Threats and Vulnerabilities			
59	⊕	Describe the difference between a cyber threat and a vulnerability.	
60	⊕	Describe types of cyber threats.	

61	⊕	Analyze types of current cyber threats.	
62	⊕	Identify the perpetrators of different types of malicious hacking.	
63	⊕	Describe the characteristics of vulnerabilities.	
64	⊕	Identify the prevention of and protections against cyber threats.	
65	○	Identify the cyber risks associated with bring your own device (BYOD) opportunities on computer networks.	
Exploring Ethics as it Relates to Cybersecurity			
66	⊕	Differentiate between ethics and laws.	
67	⊕	Distinguish among types of ethical concerns.	
68	⊕	Define *cyber bullying*.	
69	⊕	Identify actions that constitute cyber bullying.	
70	○	Identify possible warning signs of someone being cyber bullied.	
71	⊕	Identify laws applicable to cybersecurity.	
72	⊕	Explain the concept of "personally identifiable information."	
73	⊕	Explain how and why personal data is valuable to both an individual and to the organizations (e.g., governments, businesses) that collect it, analyze it, and make decisions based on it.	
74	⊕	Identify ways to control and protect personal data.	
75	○	Demonstrate net etiquette (*netiquette*) as it relates to cybersecurity.	
76	⊕	Analyze the social and legal significance of the ongoing collection of personal digital information.	
Examining Data Security as it Relates to Cybersecurity			
77	⊕	Distinguish between data, information, and knowledge.	
78	⊕	Identify the most common ways data is collected.	
79	⊕	Identify the most common ways data can be stored.	

80	⊕	Explain the difference between data at rest, data in transit, and data being processed.	
81	⊕	Identify the most common ways data is used.	
82	⊕	Discuss how data can be compromised, corrupted, or lost.	
83	⊕	Explain how businesses and individuals can protect themselves against threats to their data (e.g., firewalls, encryption, disabling, backups, permissions).	
Securing Operating Systems			
84	⊕	Define the function of a computer operating system.	
85	○	Identify the components of an operating system.	
86	⊕	List types of operating systems.	
87	⊕	Evaluate the potential vulnerabilities, threats, and common exploits to an operating system.	
88	⊕	Identify best practices for protecting operating systems.	
89	⊕	Describe the concept of malware and techniques to guard against it.	
90	⊕	Evaluate critical operating system security parameters.	
91	○	Describe security and auditing logs.	
92	○	Describe the role of a system backup.	
93	⊕	Define *virtualization technology*.	
94	○	Identify advantages and disadvantages of using virtual machines.	
Programming as a Component of Cybersecurity			
95	⊕	Define *programming* in the context of cybersecurity.	
96	⊕	Differentiate between computer programming languages.	
97	⊕	Evaluate common programming flaws that lead to vulnerabilities.	
98	⊕	Identify best practices in secure coding and design.	
Exploring Cybersecurity Implications for Current and Emerging Technologies			

99	⊕	Identify ubiquitous computing.	
100	⊕	Discuss security and privacy implications of ubiquitous computing.	
Exploring Cybersecurity Careers			
101	⊕	Research career opportunities for cybersecurity professionals.	
102	⊕	Explore the Career Clusters affected by current and emerging technology.	
103	⊕	Identify the educational pathways for emerging cybersecurity professionals.	
104	⊕	Identify career paths and job titles within the cybersecurity/cyber forensics industry and Career Clusters.	
105	⊕	Research the cyber threats and security measures related to career pathways.	
Preparing for Industry Certification			
106	⊕	Identify testing skills/strategies for a certification examination.	
107	⊕	Describe the process and requirements for obtaining industry certifications related to the Cybersecurity Fundamentals course.	
108	⊕	Demonstrate the ability to complete selected practice examinations (e.g., practice questions similar to those on certification exams).	
109	⊕	Successfully complete an industry certification examination representative of skills learned in this course (e.g., Microsoft, IC3, CompTIA).	

Legend: ⊕Essential ○Non-essential ⊖Omitted

Curriculum Framework

Exploring Cybersecurity Fundamentals

Task Number 39

Describe *cybersecurity*.

Definition

Description should state that cybersecurity is the protection of information and data —which includes information systems (e.g., networks, hardware, software), the human element, and physical elements—from risks associated with threats, attacks, hazards, or physical damage.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Global Business
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 02 Presidential Cyber Platform
  - Objective 1: Identify real-world issues related to cybersecurity.
  - Objective 2: Explain presidential power of executive order and how it was threatened in 2012.
  - Objective 3: Understand partisan politics and discuss how issues are resolved.
- 04 Current Events Project

        - Objective 1: Identify and understand current events relating to cyber.
        - Objective 2: Use MLA or APA citation formats for research report writing.
    - 05 Networks
        - Objective 1: Understand the components of a computer network.
        - Objective 2: Learn about various forms of malware and how they work.
        - Objective 3: Gain practical knowledge into network and malware functionality.
    - 06 Ethics Malware and Network Attacks
        - Objective 1: Understand networks and malware.
        - Objective 2: Analyze a practical situation concerning a computer network attack (CNA).
    - 07 Passwords
        - Objective 1: Understand common shortfalls of passwords.
        - Objective 2: Evaluate alternatives to the standard password, describe what makes a password strong, and suggest how to protect personal information online.

Cyber Literacy II

Liberal Arts

- LA02 Introduction to the 4th Amendment- Pt. 2
    - Objective 1: The learner will discuss the 4th amendment more in-depth, including a discussion on the relationship between electronic surveillance and the right to privacy.
- LA04 Fourth Amendment Project
    - Objective 1: The learner will research current Department of Justice policy on electronic search and seizure.
    - Objective 2: The learner will research current event articles on cybersecurity and privacy.
- LA07 Debate Project
    - Objective 1: The learner will participate in developing group process, persuade, compromise, debate, resolve conflicts, and negotiate differences.
    - Objective 2: The learner will synthesize facts from current events reports on national security topics such as reader privacy, government secrecy, whistleblowers, government surveillance, and prosecuting terrorist supporters.

Systems Engineering

- BB04 Programming Pushbuttons

- Objective 1: The learner will experiment with pushbuttons as input devices.
- Objective 2: The learner will display status using LEDs as output devices.

Cyber Science

Section 2

- Lesson 10 Security & Cybersecurity
  - Objective 1: The learner will define security and cybersecurity.
  - Objective 2: The learner will explore implications of security in cyberspace.

Section 4

- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 41 Security in Communications
  - Objective 1: The learner will gain an understanding of security in communications.
  - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
- Lesson 42 Political Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 43 Network Security
  - Objective 1: The learner will gain an understanding of covert channels.
  - Objective 2: The learner will gain an ability to establish a covert channel.
- Lesson 46 Civil Liberties Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 49 Man-In-The-Middle Attacks
  - Objective 1: The learner will gain an understanding of how strong public-key encryption alone does not ensure a secure communication.
  - Objective 2: The learner will investigate the importance of certificate authorities.

Section 5

- Lesson 52 Cryptography
  - Objective 1: The learner will explore basic encodings and cryptography.
  - Objective 2: The learner will gain an ability to abstract a problem to the mathematical component.
- Lesson 66 Brute Force Attacks
  - Objective 1: The learner will gain an understanding of brute force strategies, attacks, and approaches.
  - Objective 2: The learner will gain an understanding of dictionaries and their uses.
  - Objective 3: The leaner will gain an understanding of simple regular expressions.

Computer Science

- Lesson iii Introduction to Computer Science
  - Objective 1: The learner will become familiar with the Computer Science curriculum.
  - Objective 2: The learner will be introduced to computer science.
  - Objective 3: The learner will be introduced to how computers are used.
  - Objective 4: The learner will be introduced to how computer software works.
  - Objective 5: The learner will be introduced to how computer hardware works.
  - Objective 6: The learner will be introduced to the limitations and potential of computing.
- Lesson 5 Intro to Computer Architecture
  - Objective 1: The learner will be introduced to the layers of a computer system.
  - Objective 2: The learner will be introduced to the fundamentals of digital logic.
  - Objective 3: The learner will implement simple circuits (as circuit diagrams and layout diagrams) using electronic components.
  - Objective 4: The learner will implement these circuits (some as computer programs) on the Raspberry Pi.
  - Objective 5: The learner will be introduced to logic gates and truth tables.
  - Objective 6: The learner will be introduced to Boolean algebra.
  - Objective 7: The learner will be introduced to combinational circuits (including comparators).
  - Objective 8: The learner will be introduced to various form of Ohm's law.
- Lesson 7 Computer Programming in Python
  - Objective 1: The learner will be introduced to the Python programming language.

- Objective 2: The learner will be shown various difference between Scratch and Python.
- Objective 3: The learner will be introduced to various constructs, operators, and concepts in Python.
- Objective 4: The learner will write programs in Python.

Cyber Society

Law, Politics, and Terrorism

Law

- Lesson 03 Your Permanent Electronic Record
  - Objective 1: The student will identify and understand the social and legal significance of having a permanent electronic record.
  - Objective 2: The student will evaluate arguments related to legal enactments intended to mitigate the permanence of our electronic records.
  - Objective 3: The student will reflect on and develop their own understanding of the value that must be struck between the preservation of information and the protection of individuals (especially minors) from the lifelong impact of momentary choices.
- Lesson 04 Privacy vs Security
  - Objective 1: Students will identify and distinguish legal issues from other normative concerns – moral, social, etc.
  - Objective 2: Students will evaluate arguments about the value and role of law in addressing social challenges.
  - Objective 3: Students will reflect on and develop their own understanding of the impact of technology on their personal lives.

Terrorism

- Lesson 01 Definitions
  - Objective 1: The student will construct their own definitions of terrorism and cyber terrorism after interacting with multiple sources that provide examples and working definitions from private and government agencies.
  - Objective 2: The student will compare physical terrorism and cyber terrorism to identify the similarities and differences between them.
- Lesson 02 History of Terrorism
  - Objective 1: The student will classify acts of aggression throughout history as either an example of terrorism or cyber terrorism.

        - Objective 2: The student will justify the classification of acts of aggression using the definitions of terrorism and cyber terrorism.
        - Objective 3: The student will organize information given into a timeline format that includes dates, responsible party, event, and relevant information.
    - Lesson 04 Societal Responses and Consequences
        - Objective 1: The student will list five ways that the government or community members may react or respond to terrorist attacks, physical or cyber.
        - Objective 2: The student will compare and contrast a community's responses based on whether the attack was physical or in cyberspace.

Business and AI

Business

- 03 Data Threats
    - Objective 1: The student will explain the difference between data and information.
    - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
    - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
    - Objective 4: The student will explain the most common points of vulnerability.
    - Objective 5: The student will explain the most common methods of breaching computer security.
    - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.

Task Number 40

Define *information assurance*.

Definition

Definition should state that information assurance is the process that involves protecting information systems and managing the risks to systems by protecting user data through measures of confidentiality, integrity, availability, authenticity, and nonrepudiation.

Common Career Technical Core

IT9
Describe quality assurance practices and methods employed in producing and providing quality IT products and services.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Global Business
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science

Section 2

- Lesson 15 Cyber Space Opposition
  - Objective 1: The learner will begin to assess critically the Internet and cyberspace and its effect on how people think.
- Lesson 19 Cyberspace Support
  - Objective 1: The learner will understand and asses critical arguments made in favor of cyberspace's role in improving human capabilities.

Section 4

- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.

        - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 41 Security in Communications
    - Objective 1: The learner will gain an understanding of security in communications.
    - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
- Lesson 43 Network Security
    - Objective 1: The learner will gain an understanding of covert channels.
    - Objective 2: The learner will gain an ability to establish a covert channel.
- Lesson 45 Physical Security
    - Objective 1: The learner will learn about physical security and its importance.

Section 5

- Lesson 56 Cyber Privacy in Corporate World
    - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
    - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.
- Lesson 61 Digital Forensics
    - Objective 1: The learner will gain an understanding of digital forensics (DF).
    - Objective 2: The learner will gain an understanding of the forensics process.
    - Objective 3: The learner will gain a basic understanding of cybercrime.
    - Objective 4: The learner will understand the persistence of information.

Cyber Society

Business and AI

Business

- 01 Business in a Digital Age
    - Objective 1: The student will distinguish between data, information, and knowledge.
    - Objective 2: The student will describe the major information systems commonly used in business today.
    - Objective 3: The student will explain how one business function has been completely revolutionized by using digital information and technology.

- Objective 4: The student will identify 10 important characteristics of information used in businesses.
- Objective 5: The student will explain why protecting data integrity is essential to a business and the consequences of bad data.

Task Number 41

Describe the critical factors of information security.

Definition

Description should include

- explaining that the CIA triad model provides the baseline standard of evaluating and implementing information security measures on any system
- stating that each component in the CIA triad has designated goals that provide distinct requirements, and that each goal provides an essential component of information security measures
- identifying the following goals within the CIA triad and defining the terms as they apply to cybersecurity:
    - *Confidentiality*: The goal ensures that data are only accessed by authorized person(s) through security measures such as user names and passwords and access control lists (ACL).
    - *Integrity*: The goal ensures the data are trusted. This means data must be guarded against unauthorized changes. Methods of ensuring integrity include data permissions and encryption.
    - *Availability*: The goal is to provide solutions to ensure that systems can be accessed when requested. This includes providing deploying system protections and proper hardware maintenance and system patching.
    - Additional components should include the following:
        - *Authentication*: A process in which credentials are provided to verify the identity of an entity (e.g., user, system).
        - *Nonrepudiation*: A cryptologic technique that provides the proof of the integrity and origin of data.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.

Global Business

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.

Health Care Administration

Management Information Systems

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.

Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science

Section 2

- Lesson 15 Cyber Space Opposition
  - Objective 1: The learner will begin to assess critically the Internet and cyberspace and its effect on how people think.
- Lesson 19 Cyberspace Support
  - Objective 1: The learner will understand and asses critical arguments made in favor of cyberspace's role in improving human capabilities.

Section 4

- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 41 Security in Communications
  - Objective 1: The learner will gain an understanding of security in communications.
  - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
- Lesson 43 Network Security
  - Objective 1: The learner will gain an understanding of covert channels.
  - Objective 2: The learner will gain an ability to establish a covert channel.
- Lesson 45 Physical Security

- Objective 1: The learner will learn about physical security and its importance.

Section 5

- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.
- Lesson 61 Digital Forensics
  - Objective 1: The learner will gain an understanding of digital forensics (DF).
  - Objective 2: The learner will gain an understanding of the forensics process.
  - Objective 3: The learner will gain a basic understanding of cybercrime.
  - Objective 4: The learner will understand the persistence of information.

Cyber Society

Law, Politics, and Terrorism

Law

- Lesson 03 Your Permanent Electronic Record
  - Objective 1: The student will identify and understand the social and legal significance of having a permanent electronic record.
  - Objective 2: The student will evaluate arguments related to legal enactments intended to mitigate the permanence of our electronic records.
  - Objective 3: The student will reflect on and develop their own understanding of the value that must be struck between the preservation of information and the protection of individuals (especially minors) from the lifelong impact of momentary choices.
- Lesson 04 Privacy vs Security
  - Objective 1: Students will identify and distinguish legal issues from other normative concerns – moral, social, etc.
  - Objective 2: Students will evaluate arguments about the value and role of law in addressing social challenges.
  - Objective 3: Students will reflect on and develop their own understanding of the impact of technology on their personal lives.

Business and AI

Business

- 01 Business in a Digital Age
  - Objective 1: The student will distinguish between data, information, and knowledge.
  - Objective 2: The student will describe the major information systems commonly used in business today.
  - Objective 3: The student will explain how one business function has been completely revolutionized by using digital information and technology.
  - Objective 4: The student will identify 10 important characteristics of information used in businesses.
  - Objective 5: The student will explain why protecting data integrity is essential to a business and the consequences of bad data.
- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.
  - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
  - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
  - Objective 4: The student will explain the most common points of vulnerability.
  - Objective 5: The student will explain the most common methods of breaching computer security.
  - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
- 04 How Businesses Secure Information
  - Objective 1: The student will describe five kinds of security threats to an organization.
  - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
  - Objective 3: The student will explain five strategies for controlling risk.
  - Objective 4: The student will list common technologies used to improve information security.

Task Number 42

Explain cybersecurity services as they relate to intrusion prevention capabilities that protect systems against unauthorized access, exploitation, and data exfiltration.

Definition

Explanation should include the concepts that

- cybersecurity services provide the tools, methods, and procedures that a business can use to protect their systems from unauthorized access to, or the copying, transfer, or retrieval of data
- services can range from storing backups at remote sites, along with network monitoring of vulnerable software against intruders.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Global Business
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science
Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.

- Lesson 39 Networking Routers
    - Objective 1: The learner will gain an ability to setup a local area network (LAN).
    - Objective 2: The learner will gain an ability to setup a firewall.
- Lesson 40 Boe-Bot Communication
    - Objective 1: The learner will gain an ability to setup a rudimentary (daisy-chain) network using Boe-Bots.
    - Objective 2: The learner will be able to identify (one way as to) how basic information is transmitted across a wire.
- Lesson 41 Security in Communications
    - Objective 1: The learner will gain an understanding of security in communications.
    - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
- Lesson 43 Network Security
    - Objective 1: The learner will gain an understanding of covert channels.
    - Objective 2: The learner will gain an ability to establish a covert channel.
- Lesson 45 Physical Security
    - Objective 1: The learner will learn about physical security and its importance.
- Lesson 49 Man-In-The-Middle Attacks
    - Objective 1: The learner will gain an understanding of how strong public-key encryption alone does not ensure a secure communication.
    - Objective 2: The learner will investigate the importance of certificate authorities.

Cyber Society

Business and AI

Business

- 02 You Are The Data
    - Objective 1: The student will explain the concept of personal information.
    - Objective 2: The student will explain the difference between data and information.
    - Objective 3: The student will explain the most common ways that data is collected and stored.
    - Objective 4: The student will identify the common ways that they generate data in their everyday lives.
    - Objective 5: The student will explain how and why their personal data is valuable both to themselves and to governments and businesses that collect it, analyze it, and make decisions based on it.

        - Objective 6: The student will begin to control and protect their personal data.
    - 03 Data Threats
        - Objective 1: The student will explain the difference between data and information.
        - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
        - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
        - Objective 4: The student will explain the most common points of vulnerability.
        - Objective 5: The student will explain the most common methods of breaching computer security.
        - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
    - 04 How Businesses Secure Information
        - Objective 1: The student will describe five kinds of security threats to an organization.
        - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
        - Objective 3: The student will explain five strategies for controlling risk.
        - Objective 4: The student will list common technologies used to improve information security.

Task Number 43

Define *risk*.

Definition

Definition should state that risk is the likelihood that a vulnerability will occur and that a loss occurs when that vulnerability is exploited.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.

Global Business

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.

Health Care Administration

Management Information Systems

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.

Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science

Section 5

- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.

Cyber Society

Business and AI

Business

- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.
  - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
  - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
  - Objective 4: The student will explain the most common points of vulnerability.
  - Objective 5: The student will explain the most common methods of breaching computer security.
  - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.

- 04 How Businesses Secure Information
  - Objective 1: The student will describe five kinds of security threats to an organization.
  - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
  - Objective 3: The student will explain five strategies for controlling risk.
  - Objective 4: The student will list common technologies used to improve information security.

Task Number 44

Identify the concepts of cybersecurity risk management.

Definition

Identification should include

- defining risk management as the process of identifying possible vulnerabilities and quantifying potential risk as it pertains to systems
- addressing risk management strategies, including but not limited to
  - *Risk mitigation*: reducing the likelihood of the risk
  - *Risk transfer*: transferring the risk to another company, such as an insurance firm
  - *Risk avoidance*: avoiding the possibility of the risk (e.g., not using a specific software program would avoid any known risks of that program)
  - *Risk acceptance*: understanding and accepting the risks associated with use of a system or feature.

Common Career Technical Core

IT8
Recognize and analyze potential IT security threats to develop and maintain security requirements.
IT9
Describe quality assurance practices and methods employed in producing and providing quality IT products and services.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Global Business
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science
Section 5

- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.

Cyber Society
Business and AI
Business

- 04 How Businesses Secure Information
  - Objective 1: The student will describe five kinds of security threats to an organization.
  - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
  - Objective 3: The student will explain five strategies for controlling risk.
  - Objective 4: The student will list common technologies used to improve information security.

Task Number 45

Describe cybersecurity threats to an organization.

Definition

Description should include

- understanding that an action might exploit a vulnerability to breach security and cause potential harm
- understanding that threats come from many sources (e.g., insider threats, network threats, physical threats such as fire or floods, threats stemming from software systems or user actions).

Teacher resource:

- The Academic Initiative of the Cyber Innovative Center Cyber Business Module: How Businesses Secure Information

Common Career Technical Core

IT8
Recognize and analyze potential IT security threats to develop and maintain security requirements.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Global Business
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

NICERC Instructional Resources

Cyber Literacy

Cyber Literacy with Boe-Bot

Liberal Arts

- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.
- 06 Ethics Malware and Network Attacks
  - Objective 1: Understand networks and malware.
  - Objective 2: Analyze a practical situation concerning a computer network attack (CNA).

Cyber Literacy II

Liberal Arts

- LA01 Introduction to the 4th Amendment- Pt. 1
  - Objective 1: The learner will learn about historic 4th amendment cases involving rights to search and seizure.
  - Objective 2: The learner will begin to think about modern-day issues related to electronic search and seizure and how the historical aspects of the amendment are still relevant today.
- LA02 Introduction to the 4th Amendment- Pt. 2
  - Objective 1: The learner will discuss the 4th amendment more in-depth, including a discussion on the relationship between electronic surveillance and the right to privacy.
- LA04 Fourth Amendment Project
  - Objective 1: The learner will research current Department of Justice policy on electronic search and seizure.
  - Objective 2: The learner will research current event articles on cybersecurity and privacy.
- LA07 Debate Project
  - Objective 1: The learner will participate in developing group process, persuade, compromise, debate, resolve conflicts, and negotiate differences.
  - Objective 2: The learner will synthesize facts from current events reports on national security topics such as reader privacy, government secrecy, whistleblowers, government surveillance, and prosecuting terrorist supporters.

Systems Engineering

- BB04 Programming Pushbuttons

- Objective 1: The learner will experiment with pushbuttons as input devices.
- Objective 2: The learner will display status using LEDs as output devices.

- BB08 Infrared Programmable Remote
  - Objective 1: The learner will continue to experiment with IR.
  - Objective 2: The learner will program the Boe-Bot to interpret IR remote codes.
  - Objective 3: The learner will attempt to customize the Boe-Bot with the variety of buttons on the remote.

Cyber Science

Section 4

- Lesson 41 Security in Communications
  - Objective 1: The learner will gain an understanding of security in communications.
  - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
- Lesson 43 Network Security
  - Objective 1: The learner will gain an understanding of covert channels.
  - Objective 2: The learner will gain an ability to establish a covert channel.
- Lesson 45 Physical Security
  - Objective 1: The learner will learn about physical security and its importance.

Section 5

- Lesson 50 Intellectual Property & Piracy
  - Objective 1: The learner will understand the nature of intellectual property.
  - Objective 2: The learner will discuss the various challenges posed by cyberspace, particularly in the form of piracy.
- Lesson 53 Intellectual Property & Plagiarism
  - Objective 1: The learner will understand the nature of plagiarism.
  - Objective 2: The learner will discuss the ways in which cyberspace promotes and inhibits the possibility of plagiarism.
- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.

Cyber Society

Law, Politics, and Terrorism

Law

- Lesson 02 Intellectual Property
  - Objective 1: Students will identify and distinguish the personal and social value of protecting intellectual property.
  - Objective 2: Students will evaluate arguments both for and against the protection of intellectual property.
  - Objective 3: Students will reflect on and develop their own understanding of the role of law in balancing the competing interests surrounding intellectual property.
- Lesson 03 Your Permanent Electronic Record
  - Objective 1: The student will identify and understand the social and legal significance of having a permanent electronic record.
  - Objective 2: The student will evaluate arguments related to legal enactments intended to mitigate the permanence of our electronic records.
  - Objective 3: The student will reflect on and develop their own understanding of the value that must be struck between the preservation of information and the protection of individuals (especially minors) from the lifelong impact of momentary choices.
- Lesson 04 Privacy vs Security
  - Objective 1: Students will identify and distinguish legal issues from other normative concerns – moral, social, etc.
  - Objective 2: Students will evaluate arguments about the value and role of law in addressing social challenges.
  - Objective 3: Students will reflect on and develop their own understanding of the impact of technology on their personal lives.

Business and AI

Business

- 01 Business in a Digital Age
  - Objective 1: The student will distinguish between data, information, and knowledge.
  - Objective 2: The student will describe the major information systems commonly used in business today.
  - Objective 3: The student will explain how one business function has been completely revolutionized by using digital information and technology.

        - Objective 4: The student will identify 10 important characteristics of information used in businesses.
        - Objective 5: The student will explain why protecting data integrity is essential to a business and the consequences of bad data.
    - 02 You Are The Data
        - Objective 1: The student will explain the concept of personal information.
        - Objective 2: The student will explain the difference between data and information.
        - Objective 3: The student will explain the most common ways that data is collected and stored.
        - Objective 4: The student will identify the common ways that they generate data in their everyday lives.
        - Objective 5: The student will explain how and why their personal data is valuable both to themselves and to governments and businesses that collect it, analyze it, and make decisions based on it.
        - Objective 6: The student will begin to control and protect their personal data.
    - 03 Data Threats
        - Objective 1: The student will explain the difference between data and information.
        - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
        - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
        - Objective 4: The student will explain the most common points of vulnerability.
        - Objective 5: The student will explain the most common methods of breaching computer security.
        - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
    - 04 How Businesses Secure Information
        - Objective 1: The student will describe five kinds of security threats to an organization.
        - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
        - Objective 3: The student will explain five strategies for controlling risk.
        - Objective 4: The student will list common technologies used to improve information security.

Task Number 46

Explain why organizations need to manage risk.

Definition

Explanation should include the following:

- Unmanaged risk can cause loss.
- Every organization is vulnerable to common and unique types of threats.
- Organizations must identify vulnerable areas, along with the potential for actual threats, so they can plan operations to reduce the effect of those threats.
- Because all threats cannot be completely eliminated, organizations must address responses to threats and plans for continuous business operations.

Common Career Technical Core

IT8
Recognize and analyze potential IT security threats to develop and maintain security requirements.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Global Business
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science

Section 4

- Lesson 41 Security in Communications
  - Objective 1: The learner will gain an understanding of security in communications.
  - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
- Lesson 43 Network Security
  - Objective 1: The learner will gain an understanding of covert channels.
  - Objective 2: The learner will gain an ability to establish a covert channel.
- Lesson 45 Physical Security
  - Objective 1: The learner will learn about physical security and its importance.

Section 5

- Lesson 50 Intellectual Property & Piracy
  - Objective 1: The learner will understand the nature of intellectual property.
  - Objective 2: The learner will discuss the various challenges posed by cyberspace, particularly in the form of piracy.
- Lesson 53 Intellectual Property & Plagiarism
  - Objective 1: The learner will understand the nature of plagiarism.
  - Objective 2: The learner will discuss the ways in which cyberspace promotes and inhibits the possibility of plagiarism.
- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.

Cyber Society

Law, Politics, and Terrorism

Terrorism

- Lesson 03 Counterterrorism
  - Objective 1: The student will create a working definition of the word *dilemma*.
  - Objective 2: The student will apply the term *dilemma* to a unique scenario in a group where they are asked to produce a viable outcome.

        - Objective 3: The student will present their problem and solution to an international press conference (class) to see if all possible solutions were found and ultimately get the approval of everyone.
    - Lesson 04 Societal Responses and Consequences
        - Objective 1: The student will list five ways that the government or community members may react or respond to terrorist attacks, physical or cyber.
        - Objective 2: The student will compare and contrast a community's responses based on whether the attack was physical or in cyberspace.

Business and AI

Business

- 03 Data Threats
    - Objective 1: The student will explain the difference between data and information.
    - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
    - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
    - Objective 4: The student will explain the most common points of vulnerability.
    - Objective 5: The student will explain the most common methods of breaching computer security.
    - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
- 04 How Businesses Secure Information
    - Objective 1: The student will describe five kinds of security threats to an organization.
    - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
    - Objective 3: The student will explain five strategies for controlling risk.
    - Objective 4: The student will list common technologies used to improve information security.

Task Number 47

Discuss national or industry standards/regulations that relate to cybersecurity.

Definition

Discussion should include, but not be limited to, the following:

- Understanding that regulations that address security issues are requirements by a government or a business that must be followed. For example, in the health care industry, any system or user that has access to personal health information must follow the regulations set forth in the Health Insurance Portability and Accountability Act (HIPAA).
- Understanding that standards are a set of best practices that have been created to guide an organization's policies, procedures, and practices, rather than requirements to adhere to specific rules. For example, Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that accept payment cards.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Global Business
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 05 Networks

        - Objective 1: Understand the components of a computer network.
        - Objective 2: Learn about various forms of malware and how they work.
        - Objective 3: Gain practical knowledge into network and malware functionality.
    - 06 Ethics Malware and Network Attacks
        - Objective 1: Understand networks and malware.
        - Objective 2: Analyze a practical situation concerning a computer network attack (CNA).

Cyber Literacy II

Liberal Arts

- LA04 Fourth Amendment Project
    - Objective 1: The learner will research current Department of Justice policy on electronic search and seizure.
    - Objective 2: The learner will research current event articles on cybersecurity and privacy.

Systems Engineering

- BB04 Programming Pushbuttons
    - Objective 1: The learner will experiment with pushbuttons as input devices.
    - Objective 2: The learner will display status using LEDs as output devices.
- BB08 Infrared Programmable Remote
    - Objective 1: The learner will continue to experiment with IR.
    - Objective 2: The learner will program the Boe-Bot to interpret IR remote codes.
    - Objective 3: The learner will attempt to customize the Boe-Bot with the variety of buttons on the remote.

Cyber Science

Section 4

- Lesson 37 Networking Basic Concepts
    - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers
    - Objective 1: The learner will gain an ability to setup a local area network (LAN).
    - Objective 2: The learner will gain an ability to setup a firewall.
- Lesson 43 Network Security

- Objective 1: The learner will gain an understanding of covert channels.
- Objective 2: The learner will gain an ability to establish a covert channel.

Section 5

- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.
- Lesson 58 Steganography
  - Objective 1: The learner will learn about steganography and how to conceal messages within images.
  - Objective 2: The learner will perform an activity where steganography is used.

Cyber Society

Law, Politics, and Terrorism

Law

- Lesson 01 Technology and Criminal Law
  - Objective 1: Students will identify and distinguish crimes from claims of moral wrong.
  - Objective 2: Students will evaluate arguments about the nature of crime.
  - Objective 3: Students will reflect on and develop their own understanding of the sorts of uses of technology that ought to be criminal.
- Lesson 02 Intellectual Property
  - Objective 1: Students will identify and distinguish the personal and social value of protecting intellectual property.
  - Objective 2: Students will evaluate arguments both for and against the protection of intellectual property.
  - Objective 3: Students will reflect on and develop their own understanding of the role of law in balancing the competing interests surrounding intellectual property.
- Lesson 03 Your Permanent Electronic Record
  - Objective 1: The student will identify and understand the social and legal significance of having a permanent electronic record.

        - Objective 2: The student will evaluate arguments related to legal enactments intended to mitigate the permanence of our electronic records.
        - Objective 3: The student will reflect on and develop their own understanding of the value that must be struck between the preservation of information and the protection of individuals (especially minors) from the lifelong impact of momentary choices.
    - Lesson 04 Privacy vs Security
        - Objective 1: Students will identify and distinguish legal issues from other normative concerns – moral, social, etc.
        - Objective 2: Students will evaluate arguments about the value and role of law in addressing social challenges.
        - Objective 3: Students will reflect on and develop their own understanding of the impact of technology on their personal lives.

Task Number 48

Describe the cyberattack surface of various organizations.

Definition

Description should include the concepts that

- the attack surface includes all areas of an organization that can be penetrated or threatened.
- companies may have differing levels of vulnerability due to their integration of technology.

For example, a company that processes payments via an Internet site increases the vulnerability of threats against the payment processing system from attackers anywhere in the world. A company that does not collect information via the Internet would have much less vulnerability from that attack avenue.

Teacher resource:

- The Academic Initiative of the Cyber Innovative Center Cyber Business Module: How Businesses Secure Information

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Global Business
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.
- 06 Ethics Malware and Network Attacks
  - Objective 1: Understand networks and malware.
  - Objective 2: Analyze a practical situation concerning a computer network attack (CNA).

Cyber Literacy II
Systems Engineering

- BB08 Infrared Programmable Remote
  - Objective 1: The learner will continue to experiment with IR.
  - Objective 2: The learner will program the Boe-Bot to interpret IR remote codes.
  - Objective 3: The learner will attempt to customize the Boe-Bot with the variety of buttons on the remote.

Cyber Science

Section 2

- Lesson 10 Security & Cybersecurity
  - Objective 1: The learner will define security and cybersecurity.
  - Objective 2: The learner will explore implications of security in cyberspace.

Section 4

- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 41 Security in Communications
  - Objective 1: The learner will gain an understanding of security in communications.
  - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
- Lesson 43 Network Security
  - Objective 1: The learner will gain an understanding of covert channels.
  - Objective 2: The learner will gain an ability to establish a covert channel.
- Lesson 49 Man-In-The-Middle Attacks
  - Objective 1: The learner will gain an understanding of how strong public-key encryption alone does not ensure a secure communication.
  - Objective 2: The learner will investigate the importance of certificate authorities.

Section 5

- Lesson 52 Cryptography
  - Objective 1: The learner will explore basic encodings and cryptography.
  - Objective 2: The learner will gain an ability to abstract a problem to the mathematical component.
- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.
- Lesson 59 Cyberspace & Social Networks

        - Objective 1: The learner will better understand how personal communication and social networks have been effected by the rise of cyberspace interactions.
    - Lesson 66 Brute Force Attacks
        - Objective 1: The learner will gain an understanding of brute force strategies, attacks, and approaches.
        - Objective 2: The learner will gain an understanding of dictionaries and their uses.
        - Objective 3: The leaner will gain an understanding of simple regular expressions.

Cyber Society

Business and AI

Business

- 03 Data Threats
    - Objective 1: The student will explain the difference between data and information.
    - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
    - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
    - Objective 4: The student will explain the most common points of vulnerability.
    - Objective 5: The student will explain the most common methods of breaching computer security.
    - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
- 04 How Businesses Secure Information
    - Objective 1: The student will describe five kinds of security threats to an organization.
    - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
    - Objective 3: The student will explain five strategies for controlling risk.
    - Objective 4: The student will list common technologies used to improve information security.

Task Number 49

Analyze risks affecting critical infrastructure.

Definition

Analysis should include

- defining *critical infrastructure* as including assets critical to the functioning of a society and economy
- describing the 16 critical infrastructure sectors found in Presidential Policy Directive 21 and the effect their incapacitation or destruction would have on security, national economic security, national public health, and safety
- evolving threats, including, but not limited to
    - cyber threats
    - acts of terrorism
    - pandemics
    - extreme weather
    - accidents or technical failures
- relating evolving threats to the 16 critical infrastructure sectors.

For further information see Presidential Policy Directive 21.

Common Career Technical Core

IT8
Recognize and analyze potential IT security threats to develop and maintain security requirements.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Global Business
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science

Section 3

- Lesson 27 Innovation & Progress
  - Objective 1: The learner will examine assumptions about the connection between technological innovation and progress.

Section 4

- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.

Cyber Society

Law, Politics, and Terrorism

Terrorism

- Lesson 03 Counterterrorism
  - Objective 1: The student will create a working definition of the word *dilemma*.
  - Objective 2: The student will apply the term *dilemma* to a unique scenario in a group where they are asked to produce a viable outcome.
  - Objective 3: The student will present their problem and solution to an international press conference (class) to see if all possible solutions were found and ultimately get the approval of everyone.
- Lesson 04 Societal Responses and Consequences
  - Objective 1: The student will list five ways that the government or community members may react or respond to terrorist attacks, physical or cyber.
  - Objective 2: The student will compare and contrast a community's responses based on whether the attack was physical or in cyberspace.

Business and AI

Business

- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.

        - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
        - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
        - Objective 4: The student will explain the most common points of vulnerability.
        - Objective 5: The student will explain the most common methods of breaching computer security.
        - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
    - 04 How Businesses Secure Information
        - Objective 1: The student will describe five kinds of security threats to an organization.
        - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
        - Objective 3: The student will explain five strategies for controlling risk.
        - Objective 4: The student will list common technologies used to improve information security.

Examining Computer Networks as a Foundational Element of Cybersecurity

---

Task Number 50

Describe a network.

Definition

Description should include

- the purpose of a network
- the physical components of a network, including, but not limited to
    - network interface card (NIC)
    - switch

    - router/wireless router
    - wireless access point
- identifying software components of a network, including, but not limited to
    - operating systems
    - network operating systems or network operations and management
    - firewall
    - network security applications.

Common Career Technical Core

IT11
Demonstrate knowledge of the hardware components associated with information systems.
IT12
Compare key functions and applications of software and determine maintenance strategies for computer systems.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 05 Networks
    - Objective 1: Understand the components of a computer network.
    - Objective 2: Learn about various forms of malware and how they work.

- Objective 3: Gain practical knowledge into network and malware functionality.

Cyber Science

Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers
  - Objective 1: The learner will gain an ability to setup a local area network (LAN).
  - Objective 2: The learner will gain an ability to setup a firewall.
- Lesson 40 Boe-Bot Communication
  - Objective 1: The learner will gain an ability to setup a rudimentary (daisy-chain) network using Boe-Bots.
  - Objective 2: The learner will be able to identify (one way as to) how basic information is transmitted across a wire.
- Lesson 41 Security in Communications
  - Objective 1: The learner will gain an understanding of security in communications.
  - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
- Lesson 43 Network Security
  - Objective 1: The learner will gain an understanding of covert channels.
  - Objective 2: The learner will gain an ability to establish a covert channel.
- Lesson 49 Man-In-The-Middle Attacks
  - Objective 1: The learner will gain an understanding of how strong public-key encryption alone does not ensure a secure communication.
  - Objective 2: The learner will investigate the importance of certificate authorities.

Section 5

- Lesson 60 XBee Wireless
  - Objective 1: The learner will be introduced to wireless communication with Boe-Bots.
  - Objective 2: The learner will set up wireless modules on Boe-Bots.
  - Objective 3: The learner will amend the wireless programs to transmit and receive code.
  - Objective 4: The learner will compete in a maze navigation using wireless control.

Computer Science

- Lesson 5 Intro to Computer Architecture
  - Objective 1: The learner will be introduced to the layers of a computer system.
  - Objective 2: The learner will be introduced to the fundamentals of digital logic.
  - Objective 3: The learner will implement simple circuits (as circuit diagrams and layout diagrams) using electronic components.
  - Objective 4: The learner will implement these circuits (some as computer programs) on the Raspberry Pi.
  - Objective 5: The learner will be introduced to logic gates and truth tables.
  - Objective 6: The learner will be introduced to Boolean algebra.
  - Objective 7: The learner will be introduced to combinational circuits (including comparators).
  - Objective 8: The learner will be introduced to various form of Ohm's law.

Task Number 51

Describe a wired/cabled network.

Definition

Description should include the following:

- defining the term *wired/cabled network* as a network in which all components are connected with network/fiber optic cables. The most common wired networks use cables connecting a computer to Ethernet ports on a network router.
- citing examples of wired networks (e.g., copper wire, fiber optic).
- identifying IEEE 802 standards and recommended practices, particularly 802.1 and 802.3.

Common Career Technical Core

IT11
Demonstrate knowledge of the hardware components associated with information systems.
IT12
Compare key functions and applications of software and determine maintenance strategies for computer systems.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.

Cyber Science
Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers
  - Objective 1: The learner will gain an ability to setup a local area network (LAN).
  - Objective 2: The learner will gain an ability to setup a firewall.
- Lesson 40 Boe-Bot Communication
  - Objective 1: The learner will gain an ability to setup a rudimentary (daisy-chain) network using Boe-Bots.
  - Objective 2: The learner will be able to identify (one way as to) how basic information is transmitted across a wire.

Task Number 52

Describe a wireless network.

Definition

Description should include

- defining the term wireless network—a computer network in which connections are made without computer cables. The basis of wireless transmissions is radio waves. For example, radio waves connect devices such as laptops and phones to the Internet and to a business network and its applications.
- explaining 802.11 wireless local area network standards.

Common Career Technical Core

IT11
Demonstrate knowledge of the hardware components associated with information systems.
IT12
Compare key functions and applications of software and determine maintenance strategies for computer systems.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy

Cyber Literacy with Boe-Bot

Liberal Arts

- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.

Cyber Science

Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers
  - Objective 1: The learner will gain an ability to setup a local area network (LAN).
  - Objective 2: The learner will gain an ability to setup a firewall.

Section 5

- Lesson 60 XBee Wireless
  - Objective 1: The learner will be introduced to wireless communication with Boe-Bots.
  - Objective 2: The learner will set up wireless modules on Boe-Bots.
  - Objective 3: The learner will amend the wireless programs to transmit and receive code.
  - Objective 4: The learner will compete in a maze navigation using wireless control.

Task Number 53

Compare cabled/wired and wireless networks.

Definition

Comparison should include

- the cost of a network installation

- the cost to run and maintain a network
- network speed
- network reliability
- network security.

Common Career Technical Core

IT11
Demonstrate knowledge of the hardware components associated with information systems.
IT12
Compare key functions and applications of software and determine maintenance strategies for computer systems.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.

Cyber Science

Section 4

- Lesson 40 Boe-Bot Communication
  - Objective 1: The learner will gain an ability to setup a rudimentary (daisy-chain) network using Boe-Bots.
  - Objective 2: The learner will be able to identify (one way as to) how basic information is transmitted across a wire.

Section 5

- Lesson 60 XBee Wireless
  - Objective 1: The learner will be introduced to wireless communication with Boe-Bots.
  - Objective 2: The learner will set up wireless modules on Boe-Bots.
  - Objective 3: The learner will amend the wireless programs to transmit and receive code.
  - Objective 4: The learner will compete in a maze navigation using wireless control.

Task Number 54

Compare networking conceptual models.

Definition

Comparison should include the following models:

- Open Systems Interconnect (OSI): A seven-layer model that describes communication between systems. The layers are as follows:
  - Application
  - Presentation
  - Session
  - Transport
  - Network
  - Data link
  - Physical
- Internet (TCP/IP): A four-layer model that describes communication between systems. The layers are as follows:
  - Application
  - Transport
  - Internet
  - Network

Common Career Technical Core

IT6
Describe trends in emerging and evolving computer technologies and their influence on IT practices.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.

Cyber Science
Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers

        - Objective 1: The learner will gain an ability to setup a local area network (LAN).
        - Objective 2: The learner will gain an ability to setup a firewall.
    - Lesson 40 Boe-Bot Communication
        - Objective 1: The learner will gain an ability to setup a rudimentary (daisy-chain) network using Boe-Bots.
        - Objective 2: The learner will be able to identify (one way as to) how basic information is transmitted across a wire.
    - Lesson 41 Security in Communications
        - Objective 1: The learner will gain an understanding of security in communications.
        - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
    - Lesson 43 Network Security
        - Objective 1: The learner will gain an understanding of covert channels.
        - Objective 2: The learner will gain an ability to establish a covert channel.
    - Lesson 49 Man-In-The-Middle Attacks
        - Objective 1: The learner will gain an understanding of how strong public-key encryption alone does not ensure a secure communication.
        - Objective 2: The learner will investigate the importance of certificate authorities.

    Section 5

    - Lesson 60 XBee Wireless
        - Objective 1: The learner will be introduced to wireless communication with Boe-Bots.
        - Objective 2: The learner will set up wireless modules on Boe-Bots.
        - Objective 3: The learner will amend the wireless programs to transmit and receive code.
        - Objective 4: The learner will compete in a maze navigation using wireless control.

Task Number 55

Discuss services, their relationship to the OSI model, and potential vulnerabilities.

Definition

Discussion should include

- defining the term *service* as an application running on a computer.
- understanding:
    - Domain Name System (DNS)
    - email services
    - printing services
    - file distribution systems and services
    - directory services
    - web service
    - wireless sensor network.

Common Career Technical Core

IT12
Compare key functions and applications of software and determine maintenance strategies for computer systems.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science
Section 4

- Lesson 37 Networking Basic Concepts
    - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers

        - Objective 1: The learner will gain an ability to setup a local area network (LAN).
        - Objective 2: The learner will gain an ability to setup a firewall.
    - Lesson 41 Security in Communications
        - Objective 1: The learner will gain an understanding of security in communications.
        - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.

Task Number 56

Differentiate among network types.

Definition

Differentiation may include the following:

- Local Area Networks: A collection of computers, peripherals, and other devices that communicate across a network (wire, fiber optic, wireless) in a single network segment. LANs differ from WANs in their reliance on local addressing schemes and ability to operate without knowledge of neighboring networks.
    - LANs rely on local addressing and local network communications protocols (e.g., Address Resolution Protocol [ARP], IEEE 802.3 – Ethernet, IEEE 802.11 – Wireless Ethernet) that are the core differentiator between a LAN and a WAN. LANs are often characterized as being small in size, such as being contained within a room or a building.
    - LANs are frequently referred to by other terms that indicate their tendency for limited size, such as Personal Area Network (PAN), Home Area Network (HAN), or Storage Area Network (SAN).
    - LANs most commonly use addressing schemes at the data link layer (layer 2) of the OSI model (e.g., Media Access Control [MAC] addressing) for communication.
- Wide Area Networks: A network of LANs. WANs are primarily focused on routing traffic between local network segments and use technologies and protocols that differ from those employed by LANs.
    - While WANs are sometimes characterized in terms of size as having regional, national, or global scope, the difference in the technologies used is the core differentiator between LANs and WANs.
    - WANs are frequently referred to by other terms that describe the scope of a specific implementation, such as Personal Area Network (PAN), Campus Area Network (CAN), Metropolitan Area Network (MAN), or Global Area Network (GAN).

- WANs most commonly route traffic at the network layer (layer 3) of the OSI model, where routing is determined based on IP addresses and the network identifier (subnet mask).

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.

Cyber Science
Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers
  - Objective 1: The learner will gain an ability to setup a local area network (LAN).

        - Objective 2: The learner will gain an ability to setup a firewall.
    - Lesson 40 Boe-Bot Communication
        - Objective 1: The learner will gain an ability to setup a rudimentary (daisy-chain) network using Boe-Bots.
        - Objective 2: The learner will be able to identify (one way as to) how basic information is transmitted across a wire.
    - Lesson 41 Security in Communications
        - Objective 1: The learner will gain an understanding of security in communications.
        - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.

    Section 5

    - Lesson 60 XBee Wireless
        - Objective 1: The learner will be introduced to wireless communication with Boe-Bots.
        - Objective 2: The learner will set up wireless modules on Boe-Bots.
        - Objective 3: The learner will amend the wireless programs to transmit and receive code.
        - Objective 4: The learner will compete in a maze navigation using wireless control.

Task Number 57

Examine the concept of the Internet as a network of connected systems.

Definition

Examination should include a definition of the Internet, a global system of interconnected computer networks that use the Internet Protocol Suite (TCP/IP) to link billions of devices worldwide. It is a *network of networks* that consists of millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Introduction to Information Technology

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science
Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers
  - Objective 1: The learner will gain an ability to setup a local area network (LAN).
  - Objective 2: The learner will gain an ability to setup a firewall.

Task Number 58

Identify networking protocols.

Definition

Identification should include brief descriptions of:

- Dynamic Host Configuration Protocol (DHCP): a service that leases addresses to network clients
- Internet Protocol (IP): a part of the Internet protocol suite; the protocol by which data is sent from one computer to another; primarily responsible for network addressing
- Internet Control Message Protocol (ICMP): a part of the Internet suite responsible for message delivery, including but not limited to error messages
- Transmission Control Protocol (TCP): a part of the Internet protocol suite used to send data across a network; it is reliable and connection-oriented

- User Datagram Protocol (UDP): a part of the Internet protocol suite used by programs running on different computers on a network; UDP is used to send datagrams, but it is an unreliable, connectionless protocol
- HyperText Transfer Protocol (HTTP): an application-layer protocol used primarily on the Internet; a stateless and connectionless protocol
- Hypertext Transfer Protocol Secure (HTTPS): a variant of HTTP that adds a layer of security on the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection
- File Transfer Protocol (FTP): a client/server protocol used for transferring files to or exchanging files with a host computer. FTP is also the Internet standard for moving or transferring files from one computer to another using TCP or IP networks
- Post Office Protocol (POP): a type of computer networking and Internet standard protocol that extracts and retrieves email from a remote mail server for access by the host machine; used to retrieve email from portable devices.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science
Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers
  - Objective 1: The learner will gain an ability to setup a local area network (LAN).
  - Objective 2: The learner will gain an ability to setup a firewall.

Understanding Cyber Threats and Vulnerabilities

Task Number 59

Describe the difference between a cyber threat and a vulnerability.

Definition

Description should include

- defining *asset* as it relates to a secure environment (e.g., servers, data, sensitive information)
- explaining the types of threats (e.g., cyber, terrorism, pandemics, extreme weather, accidents or technical failures)
- defining *vulnerability*
- explaining
    - how a vulnerability can result in a threat
    - how eliminating vulnerabilities can eliminate a threat
    - exploits
    - how to calculate risk.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.

Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Society

Law, Politics, and Terrorism

Terrorism

- Lesson 01 Definitions
  - Objective 1: The student will construct their own definitions of terrorism and cyber terrorism after interacting with multiple sources that provide examples and working definitions from private and government agencies.
  - Objective 2: The student will compare physical terrorism and cyber terrorism to identify the similarities and differences between them.

Business and AI

Business

- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.
  - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
  - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
  - Objective 4: The student will explain the most common points of vulnerability.
  - Objective 5: The student will explain the most common methods of breaching computer security.
  - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
- 04 How Businesses Secure Information
  - Objective 1: The student will describe five kinds of security threats to an organization.
  - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
  - Objective 3: The student will explain five strategies for controlling risk.

- Objective 4: The student will list common technologies used to improve information security.

Task Number 60

Describe types of cyber threats.

Definition

Description should include, but not be limited to

- authentication (password, biometrics)
- acts of terrorism and how they present a threat
- pandemics and how they present a threat
    - About 75 percent of new human diseases are caused by microbes that originate in animals. These include HIV and AIDS, respiratory syndromes, Ebola virus disease, Marburg virus disease, Nipah virus infection and Zika virus. Several of these have spread extensively in human populations to cause a global epidemic (also known as a pandemic).
    - Population growth and expanded interactions between people, animals, and the environment over the coming decades are expected to increase the spillover of new disease threats from animals to people.
- natural disasters and an evaluation of such threats in the recent past
    - The effects of rising sea levels, more severe storms, extreme and prolonged drought conditions, and severe flooding pose a significant risk to critical infrastructure that provides essential services to the American public.
    - Ongoing and future changes to the climate have the potential to compound these risks and could have a major influence on infrastructure operations.
- accidents or technical failures
    - The potential for accidents and failures is often reached when infrastructure is pushed past its intended life
    - Unintentional failures

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy

Cyber Literacy with Boe-Bot

Liberal Arts

- 07 Passwords
  - Objective 1: Understand common shortfalls of passwords.
  - Objective 2: Evaluate alternatives to the standard password, describe what makes a password strong, and suggest how to protect personal information online.
- 10 Robots
  - Objective 1: Understand a variety of robotic applications.
  - Objective 2: Determine what kind of robot students would design if they had the resources.

Cyber Science

Section 2

- Lesson 10 Security & Cybersecurity
  - Objective 1: The learner will define security and cybersecurity.
  - Objective 2: The learner will explore implications of security in cyberspace.

Section 4

- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 41 Security in Communications
  - Objective 1: The learner will gain an understanding of security in communications.
  - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
- Lesson 43 Network Security

        - Objective 1: The learner will gain an understanding of covert channels.
        - Objective 2: The learner will gain an ability to establish a covert channel.
    - Lesson 45 Physical Security
        - Objective 1: The learner will learn about physical security and its importance.
    - Lesson 49 Man-In-The-Middle Attacks
        - Objective 1: The learner will gain an understanding of how strong public-key encryption alone does not ensure a secure communication.
        - Objective 2: The learner will investigate the importance of certificate authorities.

Cyber Society

Law, Politics, and Terrorism

Terrorism

- Lesson 01 Definitions
    - Objective 1: The student will construct their own definitions of terrorism and cyber terrorism after interacting with multiple sources that provide examples and working definitions from private and government agencies.
    - Objective 2: The student will compare physical terrorism and cyber terrorism to identify the similarities and differences between them.
- Lesson 02 History of Terrorism
    - Objective 1: The student will classify acts of aggression throughout history as either an example of terrorism or cyber terrorism.
    - Objective 2: The student will justify the classification of acts of aggression using the definitions of terrorism and cyber terrorism.
    - Objective 3: The student will organize information given into a timeline format that includes dates, responsible party, event, and relevant information.

Business and AI

Business

- 03 Data Threats
    - Objective 1: The student will explain the difference between data and information.
    - Objective 2: The student will explain the most common ways that data is collected, stored, and used.

        - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
        - Objective 4: The student will explain the most common points of vulnerability.
        - Objective 5: The student will explain the most common methods of breaching computer security.
        - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
    - 04 How Businesses Secure Information
        - Objective 1: The student will describe five kinds of security threats to an organization.
        - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
        - Objective 3: The student will explain five strategies for controlling risk.
        - Objective 4: The student will list common technologies used to improve information security.

Task Number 61

Analyze types of current cyber threats.

Definition

Analysis could include, but not be limited to, areas and types of threats related to

- physical facilities
- toys
- unmanned systems
- infrastructure
- cloud computing
- mobile devices
- automobile hacking
- chip technology
- phishing attacks
- denial of service (DOS)
- distributed denial of service (DDOS)
- malware (e.g., virus, worm, botnet, ransomware)
- medical devices
- state-sponsored hacking.

Common Career Technical Core

IT8
Recognize and analyze potential IT security threats to develop and maintain security requirements.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.
- 06 Ethics Malware and Network Attacks
  - Objective 1: Understand networks and malware.
  - Objective 2: Analyze a practical situation concerning a computer network attack (CNA).
- 07 Passwords
  - Objective 1: Understand common shortfalls of passwords.

- Objective 2: Evaluate alternatives to the standard password, describe what makes a password strong, and suggest how to protect personal information online.

Robotics

- 14 Infrared Navigation
  - Objective 1: Reintroduce students to the electromagnetic spectrum and the specific part that infrared fits.
  - Objective 2: Discuss uses for infrared.
  - Objective 3: Build and test the infrared circuit.
- 15 Infrared Navigation 2
  - Objective 1: Convert the IR detect program from the last lesson into a navigation program that will have the Boe-Bot avoiding obstacles without contacting them.
  - Objective 2: Wrap up the Boe-Bot portion of the course with four increasing challenges, culminating in the Boe-Bot being an edge detector: operating on a desk top and avoiding running off the desk.

Cyber Literacy II

Systems Engineering

- BB08 Infrared Programmable Remote
  - Objective 1: The learner will continue to experiment with IR.
  - Objective 2: The learner will program the Boe-Bot to interpret IR remote codes.
  - Objective 3: The learner will attempt to customize the Boe-Bot with the variety of buttons on the remote.

Cyber Science

Section 2

- Lesson 10 Security & Cybersecurity
  - Objective 1: The learner will define security and cybersecurity.
  - Objective 2: The learner will explore implications of security in cyberspace.

Section 4

- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 41 Security in Communications

        - Objective 1: The learner will gain an understanding of security in communications.
        - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
    - Lesson 43 Network Security
        - Objective 1: The learner will gain an understanding of covert channels.
        - Objective 2: The learner will gain an ability to establish a covert channel.
    - Lesson 45 Physical Security
        - Objective 1: The learner will learn about physical security and its importance.
    - Lesson 49 Man-In-The-Middle Attacks
        - Objective 1: The learner will gain an understanding of how strong public-key encryption alone does not ensure a secure communication.
        - Objective 2: The learner will investigate the importance of certificate authorities.

Cyber Society

Law, Politics, and Terrorism

Terrorism

- Lesson 01 Definitions
    - Objective 1: The student will construct their own definitions of terrorism and cyber terrorism after interacting with multiple sources that provide examples and working definitions from private and government agencies.
    - Objective 2: The student will compare physical terrorism and cyber terrorism to identify the similarities and differences between them.
- Lesson 02 History of Terrorism
    - Objective 1: The student will classify acts of aggression throughout history as either an example of terrorism or cyber terrorism.
    - Objective 2: The student will justify the classification of acts of aggression using the definitions of terrorism and cyber terrorism.
    - Objective 3: The student will organize information given into a timeline format that includes dates, responsible party, event, and relevant information.

Task Number 62

Identify the perpetrators of different types of malicious hacking.

Definition

Identification should include, but not be limited to

- script kiddies (an attacker who uses tools written by other people without an understanding or ability to write such programs themselves)
- professional criminals
- spammers
- hacktivists
- state-sponsored hackers (advanced persistent threat [APT])
- cyber-warriors

Common Career Technical Core

IT8
Recognize and analyze potential IT security threats to develop and maintain security requirements.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.
- 06 Ethics Malware and Network Attacks
  - Objective 1: Understand networks and malware.
  - Objective 2: Analyze a practical situation concerning a computer network attack (CNA).
- 07 Passwords
  - Objective 1: Understand common shortfalls of passwords.
  - Objective 2: Evaluate alternatives to the standard password, describe what makes a password strong, and suggest how to protect personal information online.

Cyber Literacy II

Systems Engineering

- BB08 Infrared Programmable Remote
  - Objective 1: The learner will continue to experiment with IR.
  - Objective 2: The learner will program the Boe-Bot to interpret IR remote codes.
  - Objective 3: The learner will attempt to customize the Boe-Bot with the variety of buttons on the remote.

Cyber Science

Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers
  - Objective 1: The learner will gain an ability to setup a local area network (LAN).
  - Objective 2: The learner will gain an ability to setup a firewall.
- Lesson 49 Man-In-The-Middle Attacks
  - Objective 1: The learner will gain an understanding of how strong public-key encryption alone does not ensure a secure communication.
  - Objective 2: The learner will investigate the importance of certificate authorities.

Cyber Society

Law, Politics, and Terrorism

Terrorism

- Lesson 01 Definitions
  - Objective 1: The student will construct their own definitions of terrorism and cyber terrorism after interacting with multiple sources that provide examples and working definitions from private and government agencies.
  - Objective 2: The student will compare physical terrorism and cyber terrorism to identify the similarities and differences between them.
- Lesson 02 History of Terrorism
  - Objective 1: The student will classify acts of aggression throughout history as either an example of terrorism or cyber terrorism.
  - Objective 2: The student will justify the classification of acts of aggression using the definitions of terrorism and cyber terrorism.
  - Objective 3: The student will organize information given into a timeline format that includes dates, responsible party, event, and relevant information.
- Lesson 03 Counterterrorism
  - Objective 1: The student will create a working definition of the word *dilemma*.
  - Objective 2: The student will apply the term *dilemma* to a unique scenario in a group where they are asked to produce a viable outcome.
  - Objective 3: The student will present their problem and solution to an international press conference (class) to see if all possible solutions were found and ultimately get the approval of everyone.

Task Number 63

Describe the characteristics of vulnerabilities.

Definition

Description should include

- defining the term *vulnerability* as a weakness which allows an attacker to reduce a system's information assurance
- understanding that a large number of vulnerabilities historically have been through flaws in software

- describing elements that make a system vulnerable (a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw)
- explaining the effect of a vulnerability on a system (i.e., compromised confidentiality, integrity, or availability of resources)
- discussing flaws in software that can lead to vulnerabilities, such as
    - buffer overflow or broken authentication and session management
    - injection vulnerabilities
    - input validation
    - privilege confusion
- evaluating vulnerabilities as they relate to
    - physical facilities and environment of the system or personnel working with the system
    - operational procedures, including security measures
    - business operations
    - hardware
    - software
    - communication equipment and network (individually or in combination)

Common Career Technical Core

IT8
Recognize and analyze potential IT security threats to develop and maintain security requirements.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science

Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers
  - Objective 1: The learner will gain an ability to setup a local area network (LAN).
  - Objective 2: The learner will gain an ability to setup a firewall.
- Lesson 49 Man-In-The-Middle Attacks
  - Objective 1: The learner will gain an understanding of how strong public-key encryption alone does not ensure a secure communication.
  - Objective 2: The learner will investigate the importance of certificate authorities.

Cyber Society

Law, Politics, and Terrorism

Terrorism

- Lesson 01 Definitions
  - Objective 1: The student will construct their own definitions of terrorism and cyber terrorism after interacting with multiple sources that provide examples and working definitions from private and government agencies.
  - Objective 2: The student will compare physical terrorism and cyber terrorism to identify the similarities and differences between them.
- Lesson 02 History of Terrorism
  - Objective 1: The student will classify acts of aggression throughout history as either an example of terrorism or cyber terrorism.
  - Objective 2: The student will justify the classification of acts of aggression using the definitions of terrorism and cyber terrorism.
  - Objective 3: The student will organize information given into a timeline format that includes dates, responsible party, event, and relevant information.

Business and AI

Business

- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.

        - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
        - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
        - Objective 4: The student will explain the most common points of vulnerability.
        - Objective 5: The student will explain the most common methods of breaching computer security.
        - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
    - 04 How Businesses Secure Information
        - Objective 1: The student will describe five kinds of security threats to an organization.
        - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
        - Objective 3: The student will explain five strategies for controlling risk.
        - Objective 4: The student will list common technologies used to improve information security.

Task Number 64

Identify the prevention of and protections against cyber threats.

Definition

Identification should state that preventions and protections against cyber-attacks change as the targets, vulnerabilities, and threats change. Identification should state that each vulnerability will have its own unique set of preventions and protections, and should include, but not be limited to the following:

- Network protection is often the initial line of defense (e.g., authentication, virus protection software, anti-spyware, anti-adware, firewalls).
- Operating systems and applications are critical to reducing vulnerabilities. Identification of systems maintenance measures that assist in system protection include, but should not be limited to, system updates and audits.
- Secure coding practices in database information and programming are critical to preventing injection vulnerabilities, in which an application sends untrusted data to an interpreter. Attackers use exploit injection flaws to steal data and compromise the target system. Protection measures should be evaluated in the system design and programming

phase. Addressing this concept in design and development will prevent flaws in production.
- User training will make the users aware of the potential threats due to their actions.

Common Career Technical Core

IT8
Recognize and analyze potential IT security threats to develop and maintain security requirements.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.
- 06 Ethics Malware and Network Attacks
  - Objective 1: Understand networks and malware.
  - Objective 2: Analyze a practical situation concerning a computer network attack (CNA).

- 07 Passwords
  - Objective 1: Understand common shortfalls of passwords.
  - Objective 2: Evaluate alternatives to the standard password, describe what makes a password strong, and suggest how to protect personal information online.

Cyber Science

Section 2

- Lesson 10 Security & Cybersecurity
  - Objective 1: The learner will define security and cybersecurity.
  - Objective 2: The learner will explore implications of security in cyberspace.

Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 39 Networking Routers
  - Objective 1: The learner will gain an ability to setup a local area network (LAN).
  - Objective 2: The learner will gain an ability to setup a firewall.
- Lesson 41 Security in Communications
  - Objective 1: The learner will gain an understanding of security in communications.
  - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
- Lesson 43 Network Security
  - Objective 1: The learner will gain an understanding of covert channels.
  - Objective 2: The learner will gain an ability to establish a covert channel.
- Lesson 45 Physical Security
  - Objective 1: The learner will learn about physical security and its importance.
- Lesson 49 Man-In-The-Middle Attacks
  - Objective 1: The learner will gain an understanding of how strong public-key encryption alone does not ensure a secure communication.

- Objective 2: The learner will investigate the importance of certificate authorities.

Cyber Society

Law, Politics, and Terrorism

Terrorism

- Lesson 03 Counterterrorism
  - Objective 1: The student will create a working definition of the word *dilemma*.
  - Objective 2: The student will apply the term *dilemma* to a unique scenario in a group where they are asked to produce a viable outcome.
  - Objective 3: The student will present their problem and solution to an international press conference (class) to see if all possible solutions were found and ultimately get the approval of everyone.
- Lesson 04 Societal Responses and Consequences
  - Objective 1: The student will list five ways that the government or community members may react or respond to terrorist attacks, physical or cyber.
  - Objective 2: The student will compare and contrast a community's responses based on whether the attack was physical or in cyberspace.
- Lesson 05 Culminating Activity
  - Objective 1: The student will analyze a terrorist attack to determine the motivating factors, desired outcomes for the terrorist group, consequences of the attack(s), and an appropriate counter-attack that could be applied to the given situation or group.
  - Objective 2: The student will compose an original presentation of their findings and conclusions.
  - Objective 3: The student will justify why their counter-attack will be the most effective way to resolve the conflict.
  - Objective 4: The student will evaluate presentations given by other groups.

Task Number 65

Identify the cyber risks associated with bring your own device (BYOD) opportunities on computer networks.

Definition

Identification should include the following:

- Personal devices and portable storage media can contain viruses that could compromise a network.
- The chances of malicious code on personal devices increase when antivirus, antispyware, and other security programs are not kept up to date.
- The chances of malicious code on personal devices are increased when operating systems are not kept up to date.
- Organization restrictions may be bypassed.
- Email and other types of communication can be exposed to man-in-the-middle attacks.

Common Career Technical Core

IT8
Recognize and analyze potential IT security threats to develop and maintain security requirements.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science
Section 5

- Lesson 51 Whisker Passcode
  - Objective 1: The learner will use knowledge of whiskers to simulate a passcode-locked mechanism.
  - Objective 2: The learner will use knowledge of networking activity to break the passcode.

Cyber Society

Ethics and Communities

Ethics

- Lesson 01 Digital Technology, Friendships, and Personal Relationships
  - Objective 1: Students will identify and distinguish different conceptions of friendship.
  - Objective 2: Students will evaluate arguments.
  - Objective 3: Students will reflect on and develop their own understanding of the impact of technology.
- Lesson 02 Digital Technology and Privacy
  - Objective 1: Students will identify and understand the nature and value of privacy.
  - Objective 2: Students will evaluate arguments related to the impact of emerging technologies on privacy.
  - Objective 3: Students will reflect on and develop their own understanding of the role of privacy in their own lives and the impact of technology on their privacy.
- Lesson 03 Digital Technology and the Human Personality
  - Objective 1: Students will list intellectual traits cultivated by an extensive use of digital technology.
  - Objective 2: Students will list emotional traits cultivated by an extensive use of digital technology.
  - Objective 3: Students will examine how the use of digital technology challenges the boundaries of the self.
  - Objective 4: Students will assess whether and how to revise the personal use of digital technology.
- Lesson 04 Digital Technology, Harms, and Trust
  - Objective 1: Students will list the types of harms associated with the most recent advances in new military technologies.
  - Objective 2: Students will list the types of harms associated with everyday social media and digital activities.
  - Objective 3: Students will assess the kind of trust or distrust that is warranted in using digital technologies.

Communities

- Lesson 04 Isolation in a Networked Society: Communication Technology and Deaf Culture
  - Objective 1: Students will evaluate the use of technology in the lives of people with disabilities.
  - Objective 2: Students will propose solutions to problems that people with disabilities face.

- Objective 3: Students will identify the strengths and weaknesses of some communication technologies as they role-play.

Exploring Ethics as it Relates to Cybersecurity

Task Number 66

Differentiate between ethics and laws.

Definition

Differentiation should include the following:

- Ethics are the moral principles that guide a person's conduct.
- Laws are the set of accepted rules and regulations created by appropriate authorities, such as national, state or local governments. Legal issues can include significant privacy and data security concerns, which can open up an organization to potential legal and liability risks.
- Examine the rights and protections for owners of intellectual property.

Common Career Technical Core

IT4
Demonstrate positive cyber citizenry by applying industry accepted ethical practices and behaviors.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.

Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 01 Introduction to Humanities and Cyber
  - Objective 1: Identify connections between cyber humanities, and liberal arts.
  - Objective 2: Consider cyberspace as an added dimension to our physical world.
- 08 Cyberbullying
  - Objective 1: Define and recognize cyberbullying when it occurs.
  - Objective 2: Identify actions that constitute bullying.
  - Objective 3: Identify possible warning signs of someone being cyberbullied.

Cyber Literacy II
Liberal Arts

- LA01 Introduction to the 4th Amendment- Pt. 1
  - Objective 1: The learner will learn about historic 4th amendment cases involving rights to search and seizure.
  - Objective 2: The learner will begin to think about modern-day issues related to electronic search and seizure and how the historical aspects of the amendment are still relevant today.
- LA02 Introduction to the 4th Amendment- Pt. 2
  - Objective 1: The learner will discuss the 4th amendment more in-depth, including a discussion on the relationship between electronic surveillance and the right to privacy.
- LA04 Fourth Amendment Project
  - Objective 1: The learner will research current Department of Justice policy on electronic search and seizure.
  - Objective 2: The learner will research current event articles on cybersecurity and privacy.

Cyber Science

Section 4

- Lesson 46 Civil Liberties Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.

Section 5

- Lesson 50 Intellectual Property & Piracy
  - Objective 1: The learner will understand the nature of intellectual property.
  - Objective 2: The learner will discuss the various challenges posed by cyberspace, particularly in the form of piracy.
- Lesson 53 Intellectual Property & Plagiarism
  - Objective 1: The learner will understand the nature of plagiarism.
  - Objective 2: The learner will discuss the ways in which cyberspace promotes and inhibits the possibility of plagiarism.
- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.
- Lesson 65 Who Governs?
  - Objective 1: The learner will explore the big picture of how we decide to shape our cyberspace future.
  - Objective 2: The learner will discuss which actors should have the most say in this future.

Cyber Society

Ethics and Communities

Ethics

- Lesson 01 Digital Technology, Friendships, and Personal Relationships
  - Objective 1: Students will identify and distinguish different conceptions of friendship.
  - Objective 2: Students will evaluate arguments.
  - Objective 3: Students will reflect on and develop their own understanding of the impact of technology.
- Lesson 02 Digital Technology and Privacy
  - Objective 1: Students will identify and understand the nature and value of privacy.

- Objective 2: Students will evaluate arguments related to the impact of emerging technologies on privacy.
- Objective 3: Students will reflect on and develop their own understanding of the role of privacy in their own lives and the impact of technology on their privacy.

Law, Politics, and Terrorism

Law

- Lesson 01 Technology and Criminal Law
  - Objective 1: Students will identify and distinguish crimes from claims of moral wrong.
  - Objective 2: Students will evaluate arguments about the nature of crime.
  - Objective 3: Students will reflect on and develop their own understanding of the sorts of uses of technology that ought to be criminal.
- Lesson 02 Intellectual Property
  - Objective 1: Students will identify and distinguish the personal and social value of protecting intellectual property.
  - Objective 2: Students will evaluate arguments both for and against the protection of intellectual property.
  - Objective 3: Students will reflect on and develop their own understanding of the role of law in balancing the competing interests surrounding intellectual property.

Task Number 67

Distinguish among types of ethical concerns.

Definition

Distinction should include

- describing ethical and unethical behaviors
- understanding that organizations must balance "reasonable security" with reasonable access.

Teacher resource:

- The Academic Initiative of the Cyber Innovative Center Cyber Law Module: Privacy vs. Security

Common Career Technical Core

IT3
Demonstrate the use of cross-functional teams in achieving IT project goals.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy II
Liberal Arts

- LA01 Introduction to the 4th Amendment- Pt. 1
  - Objective 1: The learner will learn about historic 4th amendment cases involving rights to search and seizure.
  - Objective 2: The learner will begin to think about modern-day issues related to electronic search and seizure and how the historical aspects of the amendment are still relevant today.
- LA02 Introduction to the 4th Amendment- Pt. 2
  - Objective 1: The learner will discuss the 4th amendment more in-depth, including a discussion on the relationship between electronic surveillance and the right to privacy.
- LA04 Fourth Amendment Project
  - Objective 1: The learner will research current Department of Justice policy on electronic search and seizure.
  - Objective 2: The learner will research current event articles on cybersecurity and privacy.

Cyber Science

Section 3

- Lesson 33 Artificial Intelligence
  - Objective 1: The learner will distinguish between the weak and strong artificial intelligence programs.
  - Objective 2: The learner will assess possible computer capabilities and functions.
- Lesson 34 Debate: Artificial Intelligence
  - Objective 1: The learner will participate in a structured and formal in-class debate.
  - Objective 2: the learner will debate issues related to artificial intelligence.

Section 4

- Lesson 46 Civil Liberties Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.

Section 5

- Lesson 50 Intellectual Property & Piracy
  - Objective 1: The learner will understand the nature of intellectual property.
  - Objective 2: The learner will discuss the various challenges posed by cyberspace, particularly in the form of piracy.
- Lesson 53 Intellectual Property & Plagiarism
  - Objective 1: The learner will understand the nature of plagiarism.
  - Objective 2: The learner will discuss the ways in which cyberspace promotes and inhibits the possibility of plagiarism.
- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.
- Lesson 65 Who Governs?
  - Objective 1: The learner will explore the big picture of how we decide to shape our cyberspace future.
  - Objective 2: The learner will discuss which actors should have the most say in this future.

Cyber Society

Ethics and Communities

Ethics

- Lesson 01 Digital Technology, Friendships, and Personal Relationships
  - Objective 1: Students will identify and distinguish different conceptions of friendship.
  - Objective 2: Students will evaluate arguments.
  - Objective 3: Students will reflect on and develop their own understanding of the impact of technology.
- Lesson 02 Digital Technology and Privacy
  - Objective 1: Students will identify and understand the nature and value of privacy.
  - Objective 2: Students will evaluate arguments related to the impact of emerging technologies on privacy.
  - Objective 3: Students will reflect on and develop their own understanding of the role of privacy in their own lives and the impact of technology on their privacy.
- Lesson 03 Digital Technology and the Human Personality
  - Objective 1: Students will list intellectual traits cultivated by an extensive use of digital technology.
  - Objective 2: Students will list emotional traits cultivated by an extensive use of digital technology.
  - Objective 3: Students will examine how the use of digital technology challenges the boundaries of the self.
  - Objective 4: Students will assess whether and how to revise the personal use of digital technology.
- Lesson 04 Digital Technology, Harms, and Trust
  - Objective 1: Students will list the types of harms associated with the most recent advances in new military technologies.
  - Objective 2: Students will list the types of harms associated with everyday social media and digital activities.
  - Objective 3: Students will assess the kind of trust or distrust that is warranted in using digital technologies.

Task Number 68

Define *cyber bullying*.

Definition

Definition should include using technology (i.e., Internet, interactive and digital technologies) to harass, embarrass, threaten, or otherwise target another person. By definition, cyber bullying involves minors; with adults, it is cyber harassment or cyber stalking.

FBLA Competitive Events and Activities Areas

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Social Media Campaign

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 08 Cyberbullying
  - Objective 1: Define and recognize cyberbullying when it occurs.
  - Objective 2: Identify actions that constitute bullying.
  - Objective 3: Identify possible warning signs of someone being cyberbullied.

Cyber Literacy II
Liberal Arts

- LA08 Cyber Bullying Case Study
  - Objective 1: The learner will gain a deeper understanding of the impact of cyberbullying on school-aged peers.
  - Objective 2: The learner will synthesize facts from current events articles into a cohesive argument against cyberbullying.

Cyber Society
Ethics and Communities
Ethics

- Lesson 04 Digital Technology, Harms, and Trust
  - Objective 1: Students will list the types of harms associated with the most recent advances in new military technologies.

- Objective 2: Students will list the types of harms associated with everyday social media and digital activities.
- Objective 3: Students will assess the kind of trust or distrust that is warranted in using digital technologies.

Task Number 69

Identify actions that constitute cyber bullying.

Definition

Identification should include

- sending content perceived as harmful by messaging, emails, and social media
- spreading rumors via email or by posting on social networking sites
- posting embarrassing pictures, videos, websites, or fake profiles.

Common Career Technical Core

IT4
Demonstrate positive cyber citizenry by applying industry accepted ethical practices and behaviors.

FBLA Competitive Events and Activities Areas

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Social Media Campaign

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 08 Cyberbullying

- Objective 1: Define and recognize cyberbullying when it occurs.
- Objective 2: Identify actions that constitute bullying.
- Objective 3: Identify possible warning signs of someone being cyberbullied.

Cyber Literacy II
Liberal Arts

- LA08 Cyber Bullying Case Study
  - Objective 1: The learner will gain a deeper understanding of the impact of cyberbullying on school-aged peers.
  - Objective 2: The learner will synthesize facts from current events articles into a cohesive argument against cyberbullying.

Cyber Society
Ethics and Communities
Ethics

- Lesson 04 Digital Technology, Harms, and Trust
  - Objective 1: Students will list the types of harms associated with the most recent advances in new military technologies.
  - Objective 2: Students will list the types of harms associated with everyday social media and digital activities.
  - Objective 3: Students will assess the kind of trust or distrust that is warranted in using digital technologies.

Task Number 70

Identify possible warning signs of someone being cyber bullied.

Definition

Identification could include signs such as

- unexpectedly not using their device or constantly using their device
- appearing nervous or uncomfortable using their device
- appearing angry, depressed, or frustrated after going online
- appearing depressed on an ongoing, regular basis
- becoming withdrawn from friends or family
- avoiding discussion of what they do or where they go online
- increasing absenteeism from school

- calling or texting to ask for permission to leave school without a justifiable excuse
- increasing stress or stress-related disorders
- falling grades.

Common Career Technical Core

IT4
Demonstrate positive cyber citizenry by applying industry accepted ethical practices and behaviors.

FBLA Competitive Events and Activities Areas

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Social Media Campaign

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 08 Cyberbullying
  - Objective 1: Define and recognize cyberbullying when it occurs.
  - Objective 2: Identify actions that constitute bullying.
  - Objective 3: Identify possible warning signs of someone being cyberbullied.

Cyber Literacy II
Liberal Arts

- LA08 Cyber Bullying Case Study
  - Objective 1: The learner will gain a deeper understanding of the impact of cyberbullying on school-aged peers.
  - Objective 2: The learner will synthesize facts from current events articles into a cohesive argument against cyberbullying.

Cyber Society
Ethics and Communities

Ethics

- Lesson 04 Digital Technology, Harms, and Trust
  - Objective 1: Students will list the types of harms associated with the most recent advances in new military technologies.
  - Objective 2: Students will list the types of harms associated with everyday social media and digital activities.
  - Objective 3: Students will assess the kind of trust or distrust that is warranted in using digital technologies.

Task Number 71

Identify laws applicable to cybersecurity.

Definition

Identification should include, but not be limited to

- national laws, regulations, policies, and/or standards
  - Privacy Act of 1974
  - Electronic Communications Privacy Act of 1986
  - Counterfeit Access Device and Computer Fraud and Abuse Act of 1984
  - Cyber Security Information Sharing Act of 2015 (CISA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Telecommunications Act of 1996
  - Gramm-Leach-Bliley Act
  - Family Educational Rights and Privacy Act (FERPA)
  - Sarbanes-Oxley Act of 2002
- international laws and standards (e.g., European Union and Information Security Directive).

FBLA Competitive Events and Activities Areas

Business Ethics

Business Law

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Social Media Campaign

NICERC Instructional Resources

Cyber Literacy

Cyber Literacy with Boe-Bot

Liberal Arts

- 08 Cyberbullying
  - Objective 1: Define and recognize cyberbullying when it occurs.
  - Objective 2: Identify actions that constitute bullying.
  - Objective 3: Identify possible warning signs of someone being cyberbullied.

Cyber Literacy II

Liberal Arts

- LA08 Cyber Bullying Case Study
  - Objective 1: The learner will gain a deeper understanding of the impact of cyberbullying on school-aged peers.
  - Objective 2: The learner will synthesize facts from current events articles into a cohesive argument against cyberbullying.

Cyber Science

Section 2

- Lesson 10 Security & Cybersecurity
  - Objective 1: The learner will define security and cybersecurity.
  - Objective 2: The learner will explore implications of security in cyberspace.

Section 4

- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 42 Political Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 46 Civil Liberties Security

- Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
- Objective 2: The learner will understand how these threats differ from those before cyberspace.

Section 5

- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.
- Lesson 59 Cyberspace & Social Networks
  - Objective 1: The learner will better understand how personal communication and social networks have been effected by the rise of cyberspace interactions.
- Lesson 65 Who Governs?
  - Objective 1: The learner will explore the big picture of how we decide to shape our cyberspace future.
  - Objective 2: The learner will discuss which actors should have the most say in this future.

Cyber Society

Ethics and Communities

Ethics

- Lesson 04 Digital Technology, Harms, and Trust
  - Objective 1: Students will list the types of harms associated with the most recent advances in new military technologies.
  - Objective 2: Students will list the types of harms associated with everyday social media and digital activities.
  - Objective 3: Students will assess the kind of trust or distrust that is warranted in using digital technologies.

Task Number 72

Explain the concept of “personally identifiable information.”

Definition

Explanation should include

- defining *personal data*
- differentiating between the meaning of data and information
- defining *digital footprint*, including *digital traces*
- listing examples of digital footprints that occur in everyday life
- analyzing digital footprint examples to interpret information about individuals
- naming the types of data individuals and businesses generate.

Teacher resource:

- The Academic Initiative of the Cyber Innovative Center Cyber Business Module: You are the Data

FBLA Competitive Events and Activities Areas

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Social Media Campaign

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 02 Presidential Cyber Platform
  - Objective 1: Identify real-world issues related to cybersecurity.
  - Objective 2: Explain presidential power of executive order and how it was threatened in 2012.
  - Objective 3: Understand partisan politics and discuss how issues are resolved.
- 03 Presidential Cyber Platform 2
  - Objective 1: Explore real world issues related to cybersecurity.
  - Objective 2: Learn about presidential power of executive order and how it was threatened in 2012.
  - Objective 3: Begin to learn about and understand partisan politics and how issues are resolved.
- 05 Networks

        - Objective 1: Understand the components of a computer network.
        - Objective 2: Learn about various forms of malware and how they work.
        - Objective 3: Gain practical knowledge into network and malware functionality.
    - 07 Passwords
        - Objective 1: Understand common shortfalls of passwords.
        - Objective 2: Evaluate alternatives to the standard password, describe what makes a password strong, and suggest how to protect personal information online.

Cyber Science

Section 1

- Lesson 04 Introduction to Cyber Science
    - Objective 1: The learner will be provided with a comprehensive context for thinking about cyberspace.
    - Objective 2: The learner will be engaged in critical thinking about issues raised by cyberspace, as well as related digital actions and behaviors.

Section 2

- Lesson 10 Security & Cybersecurity
    - Objective 1: The learner will define security and cybersecurity.
    - Objective 2: The learner will explore implications of security in cyberspace.
- Lesson 15 Cyber Space Opposition
    - Objective 1: The learner will begin to assess critically the Internet and cyberspace and its effect on how people think.
- Lesson 19 Cyberspace Support
    - Objective 1: The learner will understand and asses critical arguments made in favor of cyberspace's role in improving human capabilities.
- Lesson 23 Digital Natives or Immigrants
    - Objective 1: The learner will define and distinguish between digital natives and digital immigrants.
    - Objective 2: The learner will understand and assess whether cyberspace has proved to be a benefit or a hindrance to the education of students.

Section 3

- Lesson 27 Innovation & Progress

- Objective 1: The learner will examine assumptions about the connection between technological innovation and progress.

Section 4

- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 46 Civil Liberties Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 47 Debate: Intellectual Property
  - Objective 1: The learner will participate in a structured and formal in-class debate.
  - Objective 2: The learner will debate issues related to intellectual property.

Section 5

- Lesson 50 Intellectual Property & Piracy
  - Objective 1: The learner will understand the nature of intellectual property.
  - Objective 2: The learner will discuss the various challenges posed by cyberspace, particularly in the form of piracy.
- Lesson 53 Intellectual Property & Plagiarism
  - Objective 1: The learner will understand the nature of plagiarism.
  - Objective 2: The learner will discuss the ways in which cyberspace promotes and inhibits the possibility of plagiarism.
- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.
- Lesson 59 Cyberspace & Social Networks
  - Objective 1: The learner will better understand how personal communication and social networks have been effected by the rise of cyberspace interactions.
- Lesson 62 Digital Divide
  - Objective 1: The learner will understand the divide that still persists in access to cyberspace.

        - Objective 2: The learner will understand how this divide connects to other important political and social divisions.
    - Lesson 65 Who Governs?
        - Objective 1: The learner will explore the big picture of how we decide to shape our cyberspace future.
        - Objective 2: The learner will discuss which actors should have the most say in this future.

Cyber Society

Ethics and Communities

Ethics

- Lesson 01 Digital Technology, Friendships, and Personal Relationships
    - Objective 1: Students will identify and distinguish different conceptions of friendship.
    - Objective 2: Students will evaluate arguments.
    - Objective 3: Students will reflect on and develop their own understanding of the impact of technology.
- Lesson 02 Digital Technology and Privacy
    - Objective 1: Students will identify and understand the nature and value of privacy.
    - Objective 2: Students will evaluate arguments related to the impact of emerging technologies on privacy.
    - Objective 3: Students will reflect on and develop their own understanding of the role of privacy in their own lives and the impact of technology on their privacy.
- Lesson 03 Digital Technology and the Human Personality
    - Objective 1: Students will list intellectual traits cultivated by an extensive use of digital technology.
    - Objective 2: Students will list emotional traits cultivated by an extensive use of digital technology.
    - Objective 3: Students will examine how the use of digital technology challenges the boundaries of the self.
    - Objective 4: Students will assess whether and how to revise the personal use of digital technology.
- Lesson 04 Digital Technology, Harms, and Trust
    - Objective 1: Students will list the types of harms associated with the most recent advances in new military technologies.
    - Objective 2: Students will list the types of harms associated with everyday social media and digital activities.
    - Objective 3: Students will assess the kind of trust or distrust that is warranted in using digital technologies.

Communities

- Lesson 01 Networked Society
    - Objective 1: Students will discuss the networked society in order to understand the purpose of the networked society.
- Lesson 02 A Networked Society Provides Opportunities for Citizen Scientists
    - Objective 1: Students will evaluate, choose and defend their choice of science activities
    - Objective 2: Students will identify pros and cons of crowdsourcing information for citizen science.
    - Objective 3: Students will practice completing an online data collection activity.
    - Objective 4: Students will demonstrate the ability to work together in small group discussion and data collection.

Law, Politics, and Terrorism

Law

- Lesson 03 Your Permanent Electronic Record
    - Objective 1: The student will identify and understand the social and legal significance of having a permanent electronic record.
    - Objective 2: The student will evaluate arguments related to legal enactments intended to mitigate the permanence of our electronic records.
    - Objective 3: The student will reflect on and develop their own understanding of the value that must be struck between the preservation of information and the protection of individuals (especially minors) from the lifelong impact of momentary choices.
- Lesson 04 Privacy vs Security
    - Objective 1: Students will identify and distinguish legal issues from other normative concerns – moral, social, etc.
    - Objective 2: Students will evaluate arguments about the value and role of law in addressing social challenges.
    - Objective 3: Students will reflect on and develop their own understanding of the impact of technology on their personal lives.

Business and AI

Business

- 01 Business in a Digital Age
    - Objective 1: The student will distinguish between data, information, and knowledge.
    - Objective 2: The student will describe the major information systems commonly used in business today.

        - Objective 3: The student will explain how one business function has been completely revolutionized by using digital information and technology.
        - Objective 4: The student will identify 10 important characteristics of information used in businesses.
        - Objective 5: The student will explain why protecting data integrity is essential to a business and the consequences of bad data.
    - 02 You Are The Data
        - Objective 1: The student will explain the concept of personal information.
        - Objective 2: The student will explain the difference between data and information.
        - Objective 3: The student will explain the most common ways that data is collected and stored.
        - Objective 4: The student will identify the common ways that they generate data in their everyday lives.
        - Objective 5: The student will explain how and why their personal data is valuable both to themselves and to governments and businesses that collect it, analyze it, and make decisions based on it.
        - Objective 6: The student will begin to control and protect their personal data.
    - 03 Data Threats
        - Objective 1: The student will explain the difference between data and information.
        - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
        - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
        - Objective 4: The student will explain the most common points of vulnerability.
        - Objective 5: The student will explain the most common methods of breaching computer security.
        - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.

Task Number 73

Explain how and why personal data is valuable to both an individual and to the organizations (e.g., governments,

businesses) that collect it, analyze it, and make decisions based on it.

Definition

Explanation should include

- defining *big data* and *data mining*
- identifying where and how big data are stored and by whom
- identifying how big data are used
- explaining useful data that identifies and tracks individuals
- predicting how organizations customize communication with their target market based on an individual's digital footprint.

Teacher resource:

- National Integrated Cyber Education Research Center's Cyber Business Module: You are the Data

FBLA Competitive Events and Activities Areas

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Social Media Campaign

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 02 Presidential Cyber Platform
  - Objective 1: Identify real-world issues related to cybersecurity.
  - Objective 2: Explain presidential power of executive order and how it was threatened in 2012.
  - Objective 3: Understand partisan politics and discuss how issues are resolved.
- 03 Presidential Cyber Platform 2

        - Objective 1: Explore real world issues related to cybersecurity.
        - Objective 2: Learn about presidential power of executive order and how it was threatened in 2012.
        - Objective 3: Begin to learn about and understand partisan politics and how issues are resolved.
    - 05 Networks
        - Objective 1: Understand the components of a computer network.
        - Objective 2: Learn about various forms of malware and how they work.
        - Objective 3: Gain practical knowledge into network and malware functionality.
    - 07 Passwords
        - Objective 1: Understand common shortfalls of passwords.
        - Objective 2: Evaluate alternatives to the standard password, describe what makes a password strong, and suggest how to protect personal information online.

Cyber Science

Section 1

- Lesson 04 Introduction to Cyber Science
    - Objective 1: The learner will be provided with a comprehensive context for thinking about cyberspace.
    - Objective 2: The learner will be engaged in critical thinking about issues raised by cyberspace, as well as related digital actions and behaviors.

Section 2

- Lesson 10 Security & Cybersecurity
    - Objective 1: The learner will define security and cybersecurity.
    - Objective 2: The learner will explore implications of security in cyberspace.
- Lesson 15 Cyber Space Opposition
    - Objective 1: The learner will begin to assess critically the Internet and cyberspace and its effect on how people think.
- Lesson 19 Cyberspace Support
    - Objective 1: The learner will understand and asses critical arguments made in favor of cyberspace's role in improving human capabilities.
- Lesson 23 Digital Natives or Immigrants
    - Objective 1: The learner will define and distinguish between digital natives and digital immigrants.

- Objective 2: The learner will understand and assess whether cyberspace has proved to be a benefit or a hindrance to the education of students.

Section 3

- Lesson 27 Innovation & Progress
  - Objective 1: The learner will examine assumptions about the connection between technological innovation and progress.

Section 4

- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 46 Civil Liberties Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 47 Debate: Intellectual Property
  - Objective 1: The learner will participate in a structured and formal in-class debate.
  - Objective 2: The learner will debate issues related to intellectual property.

Section 5

- Lesson 50 Intellectual Property & Piracy
  - Objective 1: The learner will understand the nature of intellectual property.
  - Objective 2: The learner will discuss the various challenges posed by cyberspace, particularly in the form of piracy.
- Lesson 53 Intellectual Property & Plagiarism
  - Objective 1: The learner will understand the nature of plagiarism.
  - Objective 2: The learner will discuss the ways in which cyberspace promotes and inhibits the possibility of plagiarism.
- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.
- Lesson 59 Cyberspace & Social Networks

        - Objective 1: The learner will better understand how personal communication and social networks have been effected by the rise of cyberspace interactions.
    - Lesson 62 Digital Divide
        - Objective 1: The learner will understand the divide that still persists in access to cyberspace.
        - Objective 2: The learner will understand how this divide connects to other important political and social divisions.
    - Lesson 65 Who Governs?
        - Objective 1: The learner will explore the big picture of how we decide to shape our cyberspace future.
        - Objective 2: The learner will discuss which actors should have the most say in this future.

Cyber Society

Ethics and Communities

Ethics

- Lesson 01 Digital Technology, Friendships, and Personal Relationships
    - Objective 1: Students will identify and distinguish different conceptions of friendship.
    - Objective 2: Students will evaluate arguments.
    - Objective 3: Students will reflect on and develop their own understanding of the impact of technology.
- Lesson 02 Digital Technology and Privacy
    - Objective 1: Students will identify and understand the nature and value of privacy.
    - Objective 2: Students will evaluate arguments related to the impact of emerging technologies on privacy.
    - Objective 3: Students will reflect on and develop their own understanding of the role of privacy in their own lives and the impact of technology on their privacy.
- Lesson 03 Digital Technology and the Human Personality
    - Objective 1: Students will list intellectual traits cultivated by an extensive use of digital technology.
    - Objective 2: Students will list emotional traits cultivated by an extensive use of digital technology.
    - Objective 3: Students will examine how the use of digital technology challenges the boundaries of the self.
    - Objective 4: Students will assess whether and how to revise the personal use of digital technology.
- Lesson 04 Digital Technology, Harms, and Trust
    - Objective 1: Students will list the types of harms associated with the most recent advances in new military technologies.

- Objective 2: Students will list the types of harms associated with everyday social media and digital activities.
- Objective 3: Students will assess the kind of trust or distrust that is warranted in using digital technologies.

Communities

- Lesson 01 Networked Society
  - Objective 1: Students will discuss the networked society in order to understand the purpose of the networked society.
- Lesson 02 A Networked Society Provides Opportunities for Citizen Scientists
  - Objective 1: Students will evaluate, choose and defend their choice of science activities
  - Objective 2: Students will identify pros and cons of crowdsourcing information for citizen science.
  - Objective 3: Students will practice completing an online data collection activity.
  - Objective 4: Students will demonstrate the ability to work together in small group discussion and data collection.

Law, Politics, and Terrorism

Law

- Lesson 03 Your Permanent Electronic Record
  - Objective 1: The student will identify and understand the social and legal significance of having a permanent electronic record.
  - Objective 2: The student will evaluate arguments related to legal enactments intended to mitigate the permanence of our electronic records.
  - Objective 3: The student will reflect on and develop their own understanding of the value that must be struck between the preservation of information and the protection of individuals (especially minors) from the lifelong impact of momentary choices.
- Lesson 04 Privacy vs Security
  - Objective 1: Students will identify and distinguish legal issues from other normative concerns – moral, social, etc.
  - Objective 2: Students will evaluate arguments about the value and role of law in addressing social challenges.
  - Objective 3: Students will reflect on and develop their own understanding of the impact of technology on their personal lives.

Business and AI

Business

- 01 Business in a Digital Age
  - Objective 1: The student will distinguish between data, information, and knowledge.
  - Objective 2: The student will describe the major information systems commonly used in business today.
  - Objective 3: The student will explain how one business function has been completely revolutionized by using digital information and technology.
  - Objective 4: The student will identify 10 important characteristics of information used in businesses.
  - Objective 5: The student will explain why protecting data integrity is essential to a business and the consequences of bad data.
- 02 You Are The Data
  - Objective 1: The student will explain the concept of personal information.
  - Objective 2: The student will explain the difference between data and information.
  - Objective 3: The student will explain the most common ways that data is collected and stored.
  - Objective 4: The student will identify the common ways that they generate data in their everyday lives.
  - Objective 5: The student will explain how and why their personal data is valuable both to themselves and to governments and businesses that collect it, analyze it, and make decisions based on it.
  - Objective 6: The student will begin to control and protect their personal data.
- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.
  - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
  - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
  - Objective 4: The student will explain the most common points of vulnerability.
  - Objective 5: The student will explain the most common methods of breaching computer security.
  - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.

Task Number 74

Identify ways to control and protect personal data.

Definition

Identification should include

- using techniques to protect personal data (e.g., encryption, passwords, preferences on devices, location)
- distinguishing between acceptable and unacceptable data to share (e.g., social media, apps)
- comparing the risks and benefits of sharing data
- describing and locating metadata
- understanding privacy policies before installing and/or using applications.

Teacher resource:

- The Academic Initiative of the Cyber Innovative Center Cyber Business Module: You are the Data

FBLA Competitive Events and Activities Areas

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Social Media Campaign

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 02 Presidential Cyber Platform
  - Objective 1: Identify real-world issues related to cybersecurity.

        - Objective 2: Explain presidential power of executive order and how it was threatened in 2012.
        - Objective 3: Understand partisan politics and discuss how issues are resolved.
    - 03 Presidential Cyber Platform 2
        - Objective 1: Explore real world issues related to cybersecurity.
        - Objective 2: Learn about presidential power of executive order and how it was threatened in 2012.
        - Objective 3: Begin to learn about and understand partisan politics and how issues are resolved.
    - 05 Networks
        - Objective 1: Understand the components of a computer network.
        - Objective 2: Learn about various forms of malware and how they work.
        - Objective 3: Gain practical knowledge into network and malware functionality.
    - 07 Passwords
        - Objective 1: Understand common shortfalls of passwords.
        - Objective 2: Evaluate alternatives to the standard password, describe what makes a password strong, and suggest how to protect personal information online.

Cyber Science

Section 1

- Lesson 04 Introduction to Cyber Science
    - Objective 1: The learner will be provided with a comprehensive context for thinking about cyberspace.
    - Objective 2: The learner will be engaged in critical thinking about issues raised by cyberspace, as well as related digital actions and behaviors.

Section 2

- Lesson 10 Security & Cybersecurity
    - Objective 1: The learner will define security and cybersecurity.
    - Objective 2: The learner will explore implications of security in cyberspace.
- Lesson 15 Cyber Space Opposition
    - Objective 1: The learner will begin to assess critically the Internet and cyberspace and its effect on how people think.
- Lesson 19 Cyberspace Support

        - Objective 1: The learner will understand and asses critical arguments made in favor of cyberspace's role in improving human capabilities.
- Lesson 23 Digital Natives or Immigrants
    - Objective 1: The learner will define and distinguish between digital natives and digital immigrants.
    - Objective 2: The learner will understand and assess whether cyberspace has proved to be a benefit or a hindrance to the education of students.

Section 3

- Lesson 27 Innovation & Progress
    - Objective 1: The learner will examine assumptions about the connection between technological innovation and progress.

Section 4

- Lesson 38 Security
    - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
    - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 46 Civil Liberties Security
    - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
    - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 47 Debate: Intellectual Property
    - Objective 1: The learner will participate in a structured and formal in-class debate.
    - Objective 2: The learner will debate issues related to intellectual property.

Section 5

- Lesson 50 Intellectual Property & Piracy
    - Objective 1: The learner will understand the nature of intellectual property.
    - Objective 2: The learner will discuss the various challenges posed by cyberspace, particularly in the form of piracy.
- Lesson 53 Intellectual Property & Plagiarism
    - Objective 1: The learner will understand the nature of plagiarism.
    - Objective 2: The learner will discuss the ways in which cyberspace promotes and inhibits the possibility of plagiarism.
- Lesson 56 Cyber Privacy in Corporate World

        - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
        - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.
    - Lesson 59 Cyberspace & Social Networks
        - Objective 1: The learner will better understand how personal communication and social networks have been effected by the rise of cyberspace interactions.
    - Lesson 62 Digital Divide
        - Objective 1: The learner will understand the divide that still persists in access to cyberspace.
        - Objective 2: The learner will understand how this divide connects to other important political and social divisions.
    - Lesson 65 Who Governs?
        - Objective 1: The learner will explore the big picture of how we decide to shape our cyberspace future.
        - Objective 2: The learner will discuss which actors should have the most say in this future.

Cyber Society

Ethics and Communities

Ethics

- Lesson 01 Digital Technology, Friendships, and Personal Relationships
    - Objective 1: Students will identify and distinguish different conceptions of friendship.
    - Objective 2: Students will evaluate arguments.
    - Objective 3: Students will reflect on and develop their own understanding of the impact of technology.
- Lesson 02 Digital Technology and Privacy
    - Objective 1: Students will identify and understand the nature and value of privacy.
    - Objective 2: Students will evaluate arguments related to the impact of emerging technologies on privacy.
    - Objective 3: Students will reflect on and develop their own understanding of the role of privacy in their own lives and the impact of technology on their privacy.
- Lesson 03 Digital Technology and the Human Personality
    - Objective 1: Students will list intellectual traits cultivated by an extensive use of digital technology.
    - Objective 2: Students will list emotional traits cultivated by an extensive use of digital technology.
    - Objective 3: Students will examine how the use of digital technology challenges the boundaries of the self.

        - Objective 4: Students will assess whether and how to revise the personal use of digital technology.
    - Lesson 04 Digital Technology, Harms, and Trust
        - Objective 1: Students will list the types of harms associated with the most recent advances in new military technologies.
        - Objective 2: Students will list the types of harms associated with everyday social media and digital activities.
        - Objective 3: Students will assess the kind of trust or distrust that is warranted in using digital technologies.

Communities

- Lesson 01 Networked Society
    - Objective 1: Students will discuss the networked society in order to understand the purpose of the networked society.
- Lesson 02 A Networked Society Provides Opportunities for Citizen Scientists
    - Objective 1: Students will evaluate, choose and defend their choice of science activities
    - Objective 2: Students will identify pros and cons of crowdsourcing information for citizen science.
    - Objective 3: Students will practice completing an online data collection activity.
    - Objective 4: Students will demonstrate the ability to work together in small group discussion and data collection.

Law, Politics, and Terrorism

Law

- Lesson 03 Your Permanent Electronic Record
    - Objective 1: The student will identify and understand the social and legal significance of having a permanent electronic record.
    - Objective 2: The student will evaluate arguments related to legal enactments intended to mitigate the permanence of our electronic records.
    - Objective 3: The student will reflect on and develop their own understanding of the value that must be struck between the preservation of information and the protection of individuals (especially minors) from the lifelong impact of momentary choices.
- Lesson 04 Privacy vs Security
    - Objective 1: Students will identify and distinguish legal issues from other normative concerns – moral, social, etc.
    - Objective 2: Students will evaluate arguments about the value and role of law in addressing social challenges.

- Objective 3: Students will reflect on and develop their own understanding of the impact of technology on their personal lives.

Business and AI

Business

- 01 Business in a Digital Age
  - Objective 1: The student will distinguish between data, information, and knowledge.
  - Objective 2: The student will describe the major information systems commonly used in business today.
  - Objective 3: The student will explain how one business function has been completely revolutionized by using digital information and technology.
  - Objective 4: The student will identify 10 important characteristics of information used in businesses.
  - Objective 5: The student will explain why protecting data integrity is essential to a business and the consequences of bad data.
- 02 You Are The Data
  - Objective 1: The student will explain the concept of personal information.
  - Objective 2: The student will explain the difference between data and information.
  - Objective 3: The student will explain the most common ways that data is collected and stored.
  - Objective 4: The student will identify the common ways that they generate data in their everyday lives.
  - Objective 5: The student will explain how and why their personal data is valuable both to themselves and to governments and businesses that collect it, analyze it, and make decisions based on it.
  - Objective 6: The student will begin to control and protect their personal data.
- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.
  - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
  - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
  - Objective 4: The student will explain the most common points of vulnerability.

- Objective 5: The student will explain the most common methods of breaching computer security.
- Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.

Task Number 75

Demonstrate net etiquette (*netiquette*) as it relates to cybersecurity.

Definition

Demonstration should include

- not posting anything you would not say in person (remember the human)
- knowing where you are in cyberspace (different netiquette for different places)
- paying attention to the content you post (i.e., grammar, punctuation, spelling, accuracy, tone)
- sharing expert knowledge (knowing what you are talking about and asking valuable questions)
- using emotional intelligence
    - adhering to the same standards of behavior that you practice in direct, face-to-face discussions
    - respecting people's time
    - tempering emotional responses
    - respecting others' privacy
    - not abusing your power
    - forgiving other people's mistakes.

Teacher resources:

- "What do I need to know about technology?" Northern Virginia Community College
- "Netiquette," Justice Institute of British Columbia

FBLA Competitive Events and Activities Areas

Business Ethics

Cyber Security

Emerging Business Issues

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Social Media Campaign

NICERC Instructional Resources

Cyber Literacy

Cyber Literacy with Boe-Bot

Liberal Arts

- 02 Presidential Cyber Platform
  - Objective 1: Identify real-world issues related to cybersecurity.
  - Objective 2: Explain presidential power of executive order and how it was threatened in 2012.
  - Objective 3: Understand partisan politics and discuss how issues are resolved.
- 03 Presidential Cyber Platform 2
  - Objective 1: Explore real world issues related to cybersecurity.
  - Objective 2: Learn about presidential power of executive order and how it was threatened in 2012.
  - Objective 3: Begin to learn about and understand partisan politics and how issues are resolved.
- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.
- 07 Passwords
  - Objective 1: Understand common shortfalls of passwords.
  - Objective 2: Evaluate alternatives to the standard password, describe what makes a password strong, and suggest how to protect personal information online.

Cyber Science

Section 1

- Lesson 04 Introduction to Cyber Science
  - Objective 1: The learner will be provided with a comprehensive context for thinking about cyberspace.

- Objective 2: The learner will be engaged in critical thinking about issues raised by cyberspace, as well as related digital actions and behaviors.

Section 2

- Lesson 23 Digital Natives or Immigrants
  - Objective 1: The learner will define and distinguish between digital natives and digital immigrants.
  - Objective 2: The learner will understand and assess whether cyberspace has proved to be a benefit or a hindrance to the education of students.

Section 3

- Lesson 27 Innovation & Progress
  - Objective 1: The learner will examine assumptions about the connection between technological innovation and progress.

Section 5

- Lesson 62 Digital Divide
  - Objective 1: The learner will understand the divide that still persists in access to cyberspace.
  - Objective 2: The learner will understand how this divide connects to other important political and social divisions.

Task Number 76

Analyze the social and legal significance of the ongoing collection of personal digital information.

Definition

Analysis should include

- understanding the influence of your personal digital information on future career opportunities (e.g., getting into college, obtaining employment)
- researching news articles that demonstrate the effects of posting personal digital information
- interpreting the legal consequences of the collection of your personal digital information.

Teacher resource:

- The Academic Initiative of the Cyber Innovative Center Cyber Law Module: Your Permanent Electronic Record

FBLA Competitive Events and Activities Areas

Business Ethics

Business Law

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Social Media Campaign

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 02 Presidential Cyber Platform
  - Objective 1: Identify real-world issues related to cybersecurity.
  - Objective 2: Explain presidential power of executive order and how it was threatened in 2012.
  - Objective 3: Understand partisan politics and discuss how issues are resolved.
- 03 Presidential Cyber Platform 2
  - Objective 1: Explore real world issues related to cybersecurity.
  - Objective 2: Learn about presidential power of executive order and how it was threatened in 2012.
  - Objective 3: Begin to learn about and understand partisan politics and how issues are resolved.
- 05 Networks
  - Objective 1: Understand the components of a computer network.
  - Objective 2: Learn about various forms of malware and how they work.
  - Objective 3: Gain practical knowledge into network and malware functionality.
- 07 Passwords
  - Objective 1: Understand common shortfalls of passwords.

- Objective 2: Evaluate alternatives to the standard password, describe what makes a password strong, and suggest how to protect personal information online.

Cyber Science

Section 4

- Lesson 38 Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.
- Lesson 46 Civil Liberties Security
  - Objective 1: The learner will identify the threats that cyberspace poses to individuals and governments.
  - Objective 2: The learner will understand how these threats differ from those before cyberspace.

Section 5

- Lesson 56 Cyber Privacy in Corporate World
  - Objective 1: The learner will describe how corporations exploit cyberspace to increase profits.
  - Objective 2: The learner will differentiate and understand how citizens in the United States and Europe view privacy as it concerns corporations and the government.
- Lesson 59 Cyberspace & Social Networks
  - Objective 1: The learner will better understand how personal communication and social networks have been effected by the rise of cyberspace interactions.
- Lesson 65 Who Governs?
  - Objective 1: The learner will explore the big picture of how we decide to shape our cyberspace future.
  - Objective 2: The learner will discuss which actors should have the most say in this future.

Cyber Society

Law, Politics, and Terrorism

Law

- Lesson 02 Intellectual Property
  - Objective 1: Students will identify and distinguish the personal and social value of protecting intellectual property.
  - Objective 2: Students will evaluate arguments both for and against the protection of intellectual property.

        - Objective 3: Students will reflect on and develop their own understanding of the role of law in balancing the competing interests surrounding intellectual property.
    - Lesson 03 Your Permanent Electronic Record
        - Objective 1: The student will identify and understand the social and legal significance of having a permanent electronic record.
        - Objective 2: The student will evaluate arguments related to legal enactments intended to mitigate the permanence of our electronic records.
        - Objective 3: The student will reflect on and develop their own understanding of the value that must be struck between the preservation of information and the protection of individuals (especially minors) from the lifelong impact of momentary choices.
    - Lesson 04 Privacy vs Security
        - Objective 1: Students will identify and distinguish legal issues from other normative concerns – moral, social, etc.
        - Objective 2: Students will evaluate arguments about the value and role of law in addressing social challenges.
        - Objective 3: Students will reflect on and develop their own understanding of the impact of technology on their personal lives.

Examining Data Security as it Relates to Cybersecurity

Task Number 77

Distinguish between data, information, and knowledge.

Definition

Distinction should include

- Defining the term *data* (i.e., structured or unstructured, but uninterpreted)
- Defining the term *information* (i.e., structured)

- Defining the term *knowledge* (i.e., actionable information)
- Providing examples of data, information, and knowledge.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Society
Business and AI
Business

- 01 Business in a Digital Age
  - Objective 1: The student will distinguish between data, information, and knowledge.
  - Objective 2: The student will describe the major information systems commonly used in business today.
  - Objective 3: The student will explain how one business function has been completely revolutionized by using digital information and technology.
  - Objective 4: The student will identify 10 important characteristics of information used in businesses.
  - Objective 5: The student will explain why protecting data integrity is essential to a business and the consequences of bad data.

Task Number 78

Identify the most common ways data is collected.

Definition

Identification should include

- defining the term *data collection* as the process of gathering pieces of information (active versus passive, informed consent versus no consent)
- describing the types of sources where data can be collected.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Society
Business and AI
Business

- 01 Business in a Digital Age
  - Objective 1: The student will distinguish between data, information, and knowledge.
  - Objective 2: The student will describe the major information systems commonly used in business today.

        - Objective 3: The student will explain how one business function has been completely revolutionized by using digital information and technology.
        - Objective 4: The student will identify 10 important characteristics of information used in businesses.
        - Objective 5: The student will explain why protecting data integrity is essential to a business and the consequences of bad data.
    - 02 You Are The Data
        - Objective 1: The student will explain the concept of personal information.
        - Objective 2: The student will explain the difference between data and information.
        - Objective 3: The student will explain the most common ways that data is collected and stored.
        - Objective 4: The student will identify the common ways that they generate data in their everyday lives.
        - Objective 5: The student will explain how and why their personal data is valuable both to themselves and to governments and businesses that collect it, analyze it, and make decisions based on it.
        - Objective 6: The student will begin to control and protect their personal data.

Task Number 79

Identify the most common ways data can be stored.

Definition

Identification should include methodologies such as flat-file, simple database structure (i.e., spreadsheet), relational database, big data, and cloud storage.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Business Ethics

Cyber Security

Emerging Business Issues

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Society
Business and AI
Business

- 01 Business in a Digital Age
  - Objective 1: The student will distinguish between data, information, and knowledge.
  - Objective 2: The student will describe the major information systems commonly used in business today.
  - Objective 3: The student will explain how one business function has been completely revolutionized by using digital information and technology.
  - Objective 4: The student will identify 10 important characteristics of information used in businesses.
  - Objective 5: The student will explain why protecting data integrity is essential to a business and the consequences of bad data.
- 02 You Are The Data
  - Objective 1: The student will explain the concept of personal information.
  - Objective 2: The student will explain the difference between data and information.
  - Objective 3: The student will explain the most common ways that data is collected and stored.
  - Objective 4: The student will identify the common ways that they generate data in their everyday lives.
  - Objective 5: The student will explain how and why their personal data is valuable both to themselves and to governments and businesses that collect it, analyze it, and make decisions based on it.
  - Objective 6: The student will begin to control and protect their personal data.

- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.
  - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
  - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
  - Objective 4: The student will explain the most common points of vulnerability.
  - Objective 5: The student will explain the most common methods of breaching computer security.
  - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
- 04 How Businesses Secure Information
  - Objective 1: The student will describe five kinds of security threats to an organization.
  - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
  - Objective 3: The student will explain five strategies for controlling risk.
  - Objective 4: The student will list common technologies used to improve information security.

Task Number 80

Explain the difference between data at rest, data in transit, and data being processed.

Definition

Explanation should include

- defining *data at rest* (storage)
- defining *data in transit* (transmission)
- defining *data being processed* (memory)
- differentiating among each.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Society
Business and AI
Business

- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.
  - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
  - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
  - Objective 4: The student will explain the most common points of vulnerability.
  - Objective 5: The student will explain the most common methods of breaching computer security.
  - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
- 04 How Businesses Secure Information
  - Objective 1: The student will describe five kinds of security threats to an organization.
  - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
  - Objective 3: The student will explain five strategies for controlling risk.

- Objective 4: The student will list common technologies used to improve information security.

Task Number 81

Identify the most common ways data is used.

Definition

Identification should include how to extract specific information from stored data. Examples could include data filtering, data queries (including SQL), data mining, and data analytics.

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Society
Ethics and Communities
Communities

- Lesson 02 A Networked Society Provides Opportunities for Citizen Scientists
  - Objective 1: Students will evaluate, choose and defend their choice of science activities

- Objective 2: Students will identify pros and cons of crowdsourcing information for citizen science.
- Objective 3: Students will practice completing an online data collection activity.
- Objective 4: Students will demonstrate the ability to work together in small group discussion and data collection.

Business and AI

Business

- 01 Business in a Digital Age
  - Objective 1: The student will distinguish between data, information, and knowledge.
  - Objective 2: The student will describe the major information systems commonly used in business today.
  - Objective 3: The student will explain how one business function has been completely revolutionized by using digital information and technology.
  - Objective 4: The student will identify 10 important characteristics of information used in businesses.
  - Objective 5: The student will explain why protecting data integrity is essential to a business and the consequences of bad data.
- 02 You Are The Data
  - Objective 1: The student will explain the concept of personal information.
  - Objective 2: The student will explain the difference between data and information.
  - Objective 3: The student will explain the most common ways that data is collected and stored.
  - Objective 4: The student will identify the common ways that they generate data in their everyday lives.
  - Objective 5: The student will explain how and why their personal data is valuable both to themselves and to governments and businesses that collect it, analyze it, and make decisions based on it.
  - Objective 6: The student will begin to control and protect their personal data.
- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.
  - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
  - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.

        - Objective 4: The student will explain the most common points of vulnerability.
        - Objective 5: The student will explain the most common methods of breaching computer security.
        - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
    - 04 How Businesses Secure Information
        - Objective 1: The student will describe five kinds of security threats to an organization.
        - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
        - Objective 3: The student will explain five strategies for controlling risk.
        - Objective 4: The student will list common technologies used to improve information security.

Task Number 82

Discuss how data can be compromised, corrupted, or lost.

Definition

Discussion should include

- how vulnerabilities exist regardless of the state of the data (data at rest, data in transit, data being processed)
- methods by which data could be compromised (e.g., corruption, loss, SQL-injection attacks, ransomware, sabotage).

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Society

Ethics and Communities

Communities

- Lesson 02 A Networked Society Provides Opportunities for Citizen Scientists
  - Objective 1: Students will evaluate, choose and defend their choice of science activities
  - Objective 2: Students will identify pros and cons of crowdsourcing information for citizen science.
  - Objective 3: Students will practice completing an online data collection activity.
  - Objective 4: Students will demonstrate the ability to work together in small group discussion and data collection.

Business and AI

Business

- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.
  - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
  - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
  - Objective 4: The student will explain the most common points of vulnerability.
  - Objective 5: The student will explain the most common methods of breaching computer security.
  - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
- 04 How Businesses Secure Information
  - Objective 1: The student will describe five kinds of security threats to an organization.

- Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
- Objective 3: The student will explain five strategies for controlling risk.
- Objective 4: The student will list common technologies used to improve information security.

Task Number 83

Explain how businesses and individuals can protect themselves against threats to their data (e.g., firewalls, encryption, disabling, backups, permissions).

Definition

Explanation should include

- secure design principles
- security mechanisms
- examples of how data can be protected when in the following states:
    - Data at rest
        - authentication (e.g., passwords, biometrics)
        - encryption
        - permissions
        - backups
        - perimeter security (e.g., firewall, VPN)
    - Data in transit (e.g., cryptography)
    - Data being processed
        - patching
        - host hardening

FBLA Competitive Events and Activities Areas

Banking and Financial Systems

Business Ethics

Cyber Security

Emerging Business Issues
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.

Health Care Administration

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Society
Business and AI
Business

- 03 Data Threats
  - Objective 1: The student will explain the difference between data and information.
  - Objective 2: The student will explain the most common ways that data is collected, stored, and used.
  - Objective 3: The student will explain the most common perpetrators of cybersecurity attacks and why they do what they do.
  - Objective 4: The student will explain the most common points of vulnerability.
  - Objective 5: The student will explain the most common methods of breaching computer security.
  - Objective 6: The student will explain how businesses (and individuals) can protect themselves against threats to their data.
- 04 How Businesses Secure Information
  - Objective 1: The student will describe five kinds of security threats to an organization.
  - Objective 2: The student will describe five kinds of attacks an organization must defend itself against.
  - Objective 3: The student will explain five strategies for controlling risk.
  - Objective 4: The student will list common technologies used to improve information security.

Securing Operating Systems

Task Number 84

Define the function of a computer operating system.

Definition

Definition should include

- the role of the operating system (OS) in computing
- the structure of the OS
- the role of the OS in enabling applications
- a matching of hardware capabilities with the OS
- the criteria for selecting an OS.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Computer Science

- Lesson 1 Intro to Algorithms
  - Objective 1: The learner will be introduced to the concept of algorithms.
  - Objective 2: The learner will be introduced to the concept of control flow.

        - Objective 3: The learner will be introduced to to-do lists, flowcharts, and pseudocode.
        - Objective 4: The learner will be introduced to the concepts of decision and repetition;
        - Objective 5: The learner will be introduced to the concepts of efficiency and runtime.
        - Objective 6: The learner will be introduced to the concept of computer programs.
    - Lesson 3 Intro to Computer Programming
        - Objective 1: The learner will be introduced to the concept of computer programming.
        - Objective 2: The learner will be introduced to various programming constructs.
        - Objective 3: The learner will be introduced to the Scratch programming language.
    - Lesson 5 Intro to Computer Architecture
        - Objective 1: The learner will be introduced to the layers of a computer system.
        - Objective 2: The learner will be introduced to the fundamentals of digital logic.
        - Objective 3: The learner will implement simple circuits (as circuit diagrams and layout diagrams) using electronic components.
        - Objective 4: The learner will implement these circuits (some as computer programs) on the Raspberry Pi.
        - Objective 5: The learner will be introduced to logic gates and truth tables.
        - Objective 6: The learner will be introduced to Boolean algebra.
        - Objective 7: The learner will be introduced to combinational circuits (including comparators).
        - Objective 8: The learner will be introduced to various form of Ohm's law.

Task Number 85

Identify the components of an operating system.

Definition

Identification should include

- kernel
- shell
- utilities
- file system
- process management (including services)

- memory
- networking

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Computer Science

- Lesson 1 Intro to Algorithms
  - Objective 1: The learner will be introduced to the concept of algorithms.
  - Objective 2: The learner will be introduced to the concept of control flow.
  - Objective 3: The learner will be introduced to to-do lists, flowcharts, and pseudocode.
  - Objective 4: The learner will be introduced to the concepts of decision and repetition;
  - Objective 5: The learner will be introduced to the concepts of efficiency and runtime.
  - Objective 6: The learner will be introduced to the concept of computer programs.
- Lesson 3 Intro to Computer Programming
  - Objective 1: The learner will be introduced to the concept of computer programming.
  - Objective 2: The learner will be introduced to various programming constructs.
  - Objective 3: The learner will be introduced to the Scratch programming language.
- Lesson 5 Intro to Computer Architecture

- Objective 1: The learner will be introduced to the layers of a computer system.
- Objective 2: The learner will be introduced to the fundamentals of digital logic.
- Objective 3: The learner will implement simple circuits (as circuit diagrams and layout diagrams) using electronic components.
- Objective 4: The learner will implement these circuits (some as computer programs) on the Raspberry Pi.
- Objective 5: The learner will be introduced to logic gates and truth tables.
- Objective 6: The learner will be introduced to Boolean algebra.
- Objective 7: The learner will be introduced to combinational circuits (including comparators).
- Objective 8: The learner will be introduced to various form of Ohm's law.

Task Number 86

List types of operating systems.

Definition

Listing should include

- desktop
- server
- mobile
- network (network devices)

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Computer Science

- Lesson 7 Computer Programming in Python
  - Objective 1: The learner will be introduced to the Python programming language.
  - Objective 2: The learner will be shown various difference between Scratch and Python.
  - Objective 3: The learner will be introduced to various constructs, operators, and concepts in Python.
  - Objective 4: The learner will write programs in Python.

Task Number 87

Evaluate the potential vulnerabilities, threats, and common exploits to an operating system.

Definition

Evaluation should include the flaws to an operating system and the current and emerging threats, such as viruses, dynamic-link library (DLL) injection, or zero-day vulnerability.

Common Career Technical Core

IT8
Recognize and analyze potential IT security threats to develop and maintain security requirements.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 88

Identify best practices for protecting operating systems.

Definition

Identification should include patch management, application updates, and OS hardening.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 89

Describe the concept of malware and techniques to guard against it.

Definition

Description should include

- the types of malware and the ways they propagate
- the role of anti-virus/anti-spyware utilities
- distinguishing between available anti-virus/anti-spyware utilities
- current and emerging techniques.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science
Section 4

- Lesson 37 Networking Basic Concepts
  - Objective 1: The learner will examine how computer communicate in cyberspace.
- Lesson 39 Networking Routers
  - Objective 1: The learner will gain an ability to setup a local area network (LAN).

        - Objective 2: The learner will gain an ability to setup a firewall.
    - Lesson 41 Security in Communications
        - Objective 1: The learner will gain an understanding of security in communications.
        - Objective 2: The learner will gain an understanding of man-in-the-middle (MiM) attacks.
    - Lesson 43 Network Security
        - Objective 1: The learner will gain an understanding of covert channels.
        - Objective 2: The learner will gain an ability to establish a covert channel.
    - Lesson 45 Physical Security
        - Objective 1: The learner will learn about physical security and its importance.
    - Lesson 49 Man-In-The-Middle Attacks
        - Objective 1: The learner will gain an understanding of how strong public-key encryption alone does not ensure a secure communication.
        - Objective 2: The learner will investigate the importance of certificate authorities.

Task Number 90

Evaluate critical operating system security parameters.

Definition

Evaluation should include establishing or following

- authentication policy
- access control (rights and permissions)
- audit policy.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 91

Describe security and auditing logs.

Definition

Description should include the types of logs, with a definition and purpose for each.

Common Career Technical Core

IT10
Describe the use of computer forensics to prevent and solve information technology crimes and security breaches.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Introduction to Information Technology

Management Information Systems

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 92

Describe the role of a system backup.

Definition

Description should include

- types of backups (i.e., full, incremental, and differential)
- backup locations (e.g., media, cloud)
- discussion of the value of a backup as it relates to security.

Common Career Technical Core

IT7
Perform standard computer backup and restore procedures to protect IT information.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Cyber Security

Health Care Administration

Help Desk

Introduction to Information Technology

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 93

Define *virtualization technology*.

Definition

Definition should include, but not be limited to

- virtualization services
- what a virtual machine is and how it can be used as a sandbox
- how virtual machines relate to one another
- how hardware use is managed by virtual machines
- key properties of virtual machines
    - partitioning
    - isolation
    - encapsulation
    - hardware independence
- advantages and disadvantages of virtualization technology
- examples of virtualization platforms (hyper-V, VMWare, virtual box).

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Introduction to Information Technology

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 94

Identify advantages and disadvantages of using virtual machines.

Definition

Identification of advantages should include, but not be limited to

- reduced cost in
  - capital expenditure
  - energy expenditure
  - operational expenditure
- consolidation of resources
  - physical server consolidation (maximum server utilization, minimum server count)
  - management of server consolidation
  - many applications on each server
  - multiple operating systems can exist, isolated from each other, on the same virtual server
- isolation:
  - if one virtual server has a software failure, others are not affected
  - upgrades and changes can be made only where required.

Identification of disadvantages should include, but not be limited to

- efficiency:
  - virtual machines are not as efficient in accessing hardware as a real machine
  - when multiple virtual machines are running on a host computer, each virtual machine may introduce unstable performance to the host and thus affect the other virtual machine's applications
- cost:
  - software for virtual machines may cost more due to the expense of virtualization software
  - additional software management tools may be required
- compatibility (not all servers and applications are virtualization-friendly)
- complex root-cause analysis.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Introduction to Information Technology

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Programming as a Component of Cybersecurity

Task Number 95

Define *programming* in the context of cybersecurity.

Definition

Definition should include

- describing what a program is
- synthesizing the concept of programming as being central to the computing infrastructure
- describing what secure coding is
- citing examples of security mechanisms that are software programs.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Introduction to Information Technology

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Science
Section 5

- Lesson 54 Boe-Bot Cryptography
  - Objective 1: The learner will gain an ability to use the Boe-Bot in cryptography.
  - Objective 2: The learner will gain an understanding of basic cryptography.
- Lesson 58 Steganography
  - Objective 1: The learner will learn about steganography and how to conceal messages within images.
  - Objective 2: The learner will perform an activity where steganography is used.
- Lesson 62 Digital Divide
  - Objective 1: The learner will understand the divide that still persists in access to cyberspace.
  - Objective 2: The learner will understand how this divide connects to other important political and social divisions.

Computer Science

- Lesson 9 Recursion

- Objective 1: The learner will be introduced to the Tower of Hanoi.
- Objective 2: The learner will be introduced to breaking problems down and recurrence relations.
- Objective 3: The learner will be introduced to recursion and famous recursive algorithms.

Task Number 96

Differentiate between computer programming languages.

Definition

Differentiation should include

- compiled languages
- interpreted languages (scripting)
- rendered languages.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Introduction to Information Technology

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Computer Science

- Lesson 7 Computer Programming in Python
  - Objective 1: The learner will be introduced to the Python programming language.
  - Objective 2: The learner will be shown various difference between Scratch and Python.
  - Objective 3: The learner will be introduced to various constructs, operators, and concepts in Python.
  - Objective 4: The learner will write programs in Python.

Task Number 97

Evaluate common programming flaws that lead to vulnerabilities.

Definition

Evaluation should include the concept that other programmers can change coding, scripts, or algorithms in any computer program. Evaluation also should include a discussion of flaws in software that can lead to vulnerabilities, such as

- buffer overflow
- broken authentication and session management
- injection vulnerabilities
- input validation
- privilege confusion.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Introduction to Information Technology

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 98

Identify best practices in secure coding and design.

Definition

Identification should include, but not be limited to

- input validation
- data sanitization
- secure design principle.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Introduction to Information Technology

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Exploring Cybersecurity Implications for Current and Emerging Technologies

Task Number 99

Identify ubiquitous computing.

Definition

Identification should include, but not be limited to

- Internet of Things (IoT)
- unmanned systems
- artificial intelligence.

Common Career Technical Core

IT6
Describe trends in emerging and evolving computer technologies and their influence on IT practices.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Introduction to Information Technology

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy

Cyber Literacy with Boe-Bot

Liberal Arts

- 01 Introduction to Humanities and Cyber
  - Objective 1: Identify connections between cyber humanities, and liberal arts.
  - Objective 2: Consider cyberspace as an added dimension to our physical world.
- 04 Current Events Project
  - Objective 1: Identify and understand current events relating to cyber.
  - Objective 2: Use MLA or APA citation formats for research report writing.
- 09 Debates
  - Objective 1: Prepare for and deliver an academic debate.
  - Objective 2: Demonstrate proper MLA or other citation styles.
  - Objective 3: Prepare fact-based material for a presentation and deliver the material to a group of peers.
- 10 Robots
  - Objective 1: Understand a variety of robotic applications.
  - Objective 2: Determine what kind of robot students would design if they had the resources.

Cyber Literacy II

Liberal Arts

- LA01 Introduction to the 4th Amendment- Pt. 1
  - Objective 1: The learner will learn about historic 4th amendment cases involving rights to search and seizure.
  - Objective 2: The learner will begin to think about modern-day issues related to electronic search and seizure and how the historical aspects of the amendment are still relevant today.
- LA02 Introduction to the 4th Amendment- Pt. 2

- Objective 1: The learner will discuss the 4th amendment more in-depth, including a discussion on the relationship between electronic surveillance and the right to privacy.

Systems Engineering

- BB08 Infrared Programmable Remote
  - Objective 1: The learner will continue to experiment with IR.
  - Objective 2: The learner will program the Boe-Bot to interpret IR remote codes.
  - Objective 3: The learner will attempt to customize the Boe-Bot with the variety of buttons on the remote.
- BB10 Moon Rover
  - Objective 1: The learner will compete in a timed challenge to apply knowledge gained from BB09.
  - Objective 2: The learner will use an accelerometer to aid their Boe-Bot in becoming an autonomous navigator.
- BB15 Minefield Challenge
  - Objective 1: The learner will participate in a series of challenges designed to test multiple sensory systems

---

Task Number 100

Discuss security and privacy implications of ubiquitous computing.

Definition

Discussion should include examples of security and privacy issues in ubiquitous computing, such as IoT in smart homes.

Common Career Technical Core

IT6
Describe trends in emerging and evolving computer technologies and their influence on IT practices.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Health Care Administration

Help Desk

Introduction to Information Technology

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 01 Introduction to Humanities and Cyber
  - Objective 1: Identify connections between cyber humanities, and liberal arts.
  - Objective 2: Consider cyberspace as an added dimension to our physical world.
- 04 Current Events Project
  - Objective 1: Identify and understand current events relating to cyber.
  - Objective 2: Use MLA or APA citation formats for research report writing.
- 09 Debates
  - Objective 1: Prepare for and deliver an academic debate.
  - Objective 2: Demonstrate proper MLA or other citation styles.
  - Objective 3: Prepare fact-based material for a presentation and deliver the material to a group of peers.
- 10 Robots
  - Objective 1: Understand a variety of robotic applications.
  - Objective 2: Determine what kind of robot students would design if they had the resources.

Cyber Literacy II

Liberal Arts

- LA01 Introduction to the 4th Amendment- Pt. 1
  - Objective 1: The learner will learn about historic 4th amendment cases involving rights to search and seizure.
  - Objective 2: The learner will begin to think about modern-day issues related to electronic search and seizure and how the historical aspects of the amendment are still relevant today.
- LA02 Introduction to the 4th Amendment- Pt. 2
  - Objective 1: The learner will discuss the 4th amendment more in-depth, including a discussion on the relationship between electronic surveillance and the right to privacy.

Systems Engineering

- BB08 Infrared Programmable Remote
  - Objective 1: The learner will continue to experiment with IR.
  - Objective 2: The learner will program the Boe-Bot to interpret IR remote codes.
  - Objective 3: The learner will attempt to customize the Boe-Bot with the variety of buttons on the remote.
- BB10 Moon Rover
  - Objective 1: The learner will compete in a timed challenge to apply knowledge gained from BB09.
  - Objective 2: The learner will use an accelerometer to aid their Boe-Bot in becoming an autonomous navigator.
- BB15 Minefield Challenge
  - Objective 1: The learner will participate in a series of challenges designed to test multiple sensory systems

---

Exploring Cybersecurity Careers

Task Number 101

Research career opportunities for cybersecurity professionals.

Definition

Research should include using online job research and job posting sites (e.g., Virginia Employment Commission, CyberSeek, O*Net OnLine) to locate entry-level cybersecurity and cyber forensics opportunities at the local, state, national, and international levels.

Resource: Virginia Space Grant Consortium's free video series, "Breaking the Code on a Career in Cybersecurity," which features interviews with cyber professionals about their career pathways.

FBLA Competitive Events and Activities Areas

Cyber Security

Electronic Career Portfolio

Future Business Leader

Job Interview

Task Number 102

Explore the Career Clusters affected by current and emerging technology.

Definition

Exploration should include, but not be limited to, the following, with examples of each:

- Agriculture, Food, and Natural Resources
- Architecture and Construction
- Arts, A/V, Technology and Communications
- Business Management and Administration
- Education and Training
- Finance
- Government and Public Information
- Health Science
- Hospitality and Tourism
- Human Services
- Information Technology
- Law, Public Safety, Corrections, and Security
- Manufacturing

- Marketing
- Science, Technology, Engineering, and Mathematics
- Transportation, Distribution, and Logistics

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Electronic Career Portfolio

Health Care Administration

Help Desk

Introduction to Information Technology

Job Interview

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 103

Identify the educational pathways for emerging cybersecurity professionals.

Definition

Identification should include

- online resources that specialize in providing this type of information (e.g., O*Net Online, Bureau of Labor Statistics' Occupational Outlook Handbook, Virginia Education Wizard, CyberSeek, Cyber Innovation Center)

- common pathways based on industry requirements (i.e., internships, community college, or four-year university)
- academic goals (e.g., strong mathematics skills)
- career and technical education goals (i.e., industry certifications and licensure)
- postsecondary options (i.e., internships, community college, technical institutes, or four-year universities).

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Electronic Career Portfolio

Health Care Administration

Help Desk

Introduction to Information Technology

Job Interview

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 104

Identify career paths and job titles within the cybersecurity/cyber forensics industry and Career Clusters.

Definition

Identification should include

- related Career Clusters (e.g., Government and Public Administration; Information Technology; Law, Public Safety, Corrections and Security; Science, Technology, Engineering and Mathematics)
- Career pathways related to selected Career Clusters (for examples, see CyberSeek)
- job titles related to selected paths (e.g., cyber defenders, cyber sleuths, information security analyst, network administrator, cybersecurity researcher).

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Electronic Career Portfolio

Health Care Administration

Help Desk

Introduction to Information Technology

Job Interview

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 105

Research the cyber threats and security measures related to career pathways.

Definition

Research should include

- viruses, worms, and Trojan horses
- brute-force attacks
- privacy invasion tools (e.g., spyware, malware, ransomware, cookies, adware, and popups)
- spam.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Electronic Career Portfolio

Health Care Administration

Help Desk

Introduction to Information Technology

Job Interview

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

NICERC Instructional Resources

Cyber Literacy
Cyber Literacy with Boe-Bot
Liberal Arts

- 04 Current Events Project
  - Objective 1: Identify and understand current events relating to cyber.
  - Objective 2: Use MLA or APA citation formats for research report writing.
- 09 Debates

- Objective 1: Prepare for and deliver an academic debate.
- Objective 2: Demonstrate proper MLA or other citation styles.
- Objective 3: Prepare fact-based material for a presentation and deliver the material to a group of peers.

Preparing for Industry Certification

Task Number 106

Identify testing skills/strategies for a certification examination.

Definition

The identification of testing skills and strategies should be undertaken by

- conducting an Internet research project
- reviewing materials from publishers
- interviewing certified instructors and/or industry-certified professionals.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Electronic Career Portfolio

Health Care Administration

Help Desk

Introduction to Information Technology

Job Interview

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 107

Describe the process and requirements for obtaining industry certifications related to the Cybersecurity Fundamentals course.

Definition

Description should include a list of industry certifications related to the Cybersecurity Fundamentals course and the process/requirements for obtaining the certifications from

- official websites of the testing organization/vendor
- materials from publishers that have developed practice materials and tests based on information from the testing organization/provider
- information from certified instructors or industry-certified professionals
- information in the “Introduction/Course Description” section of this document.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Electronic Career Portfolio

Job Interview

Management Information Systems

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

Task Number 108

Demonstrate the ability to complete selected practice examinations (e.g., practice questions similar to those on certification exams).

Definition

The demonstration should include obtaining and successfully completing practice examinations for selected certifications related to the course. Practice examinations may be obtained from provider sites and/or materials from publishers. The level of performance on a practice examination serves as a gauge of the applicant's readiness for formal industry testing.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Electronic Career Portfolio

Health Care Administration

Help Desk

Introduction to Information Technology

Job Interview

Management Information Systems
The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.

Network Design

Networking Concepts

Task Number 109

Successfully complete an industry certification examination representative of skills learned in this course (e.g., Microsoft, IC3, CompTIA).

Definition

The successful completion of an industry certification examination will be achieved when the student applicant earns an examination score deemed "passing" by the testing organization. Qualifying examinations are those currently approved at the state level as representative of Cybersecurity Fundamentals skills.

Students should be encouraged to attain industry certification as evidence of their computer application skill level and general employability.

FBLA Competitive Events and Activities Areas

Business Ethics

Computer Game & Simulation Programming

Computer Problem Solving

Cyber Security

Electronic Career Portfolio

Health Care Administration

Help Desk

Introduction to Information Technology

Job Interview

Management Information Systems

The topic for this event changes from year to year. The annual topic may or may not correlate with this particular course. Please refer to the current Virginia FBLA State Handbook.
Network Design

Networking Concepts

SOL Correlation by Task

39	Describe *cybersecurity*.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14
40	Define *information assurance*.	English: 9.3, 10.3, 11.3, 12.3 History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14
41	Describe the critical factors of information security.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5 History and Social Science: GOVT.12, GOVT.16, VUS.14 Mathematics: COM.1
42	Explain cybersecurity services as they relate to intrusion prevention capabilities that protect systems against unauthorized access, exploitation, and data exfiltration.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: VUS.14 Mathematics: COM.16
43	Define *risk*.	English: 9.3, 10.3, 11.3, 12.3 History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14

44	Identify the concepts of cybersecurity risk management.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14
45	Describe cybersecurity threats to an organization.	English: 9.5, 10.5, 11.5, 12.5
46	Explain why organizations need to manage risk.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14
47	Discuss national or industry standards/regulations that relate to cybersecurity.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: GOVT.9, GOVT.16, VUS.13, VUS.14
48	Describe the cyberattack surface of various organizations.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: VUS.13, VUS.14
49	Analyze risks affecting critical infrastructure.	English: 9.3, 9.5, 9.8, 10.3, 10.5, 10.8, 11.3, 11.5, 11.8, 12.3, 12.5, 12.8 History and Social Science: GOVT.12, GOVT.16, VUS.13, VUS.14, WHII.14
50	Describe a network.	English: 9.5, 10.5, 11.5, 12.5
51	Describe a wired/cabled network.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5
52	Describe a wireless network.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5 History and Social Science: VUS.14
53	Compare cabled/wired and wireless networks.	History and Social Science: VUS.14 Mathematics: A.4, A.9, AII.9, AII.10

54	Compare networking conceptual models.	
55	Discuss services, their relationship to the OSI model, and potential vulnerabilities.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5 History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14
56	Differentiate among network types.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: VUS.14
57	Examine the concept of the Internet as a network of connected systems.	English: 9.2, 9.5, 10.2, 10.5, 11.2, 11.5, 12.2, 12.5 History and Social Science: VUS.13, WHII.14
58	Identify networking protocols.	English: 9.5, 10.5, 11.5, 12.5
59	Describe the difference between a cyber threat and a vulnerability.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5 History and Social Science: GOVT.12, GOVT.16, VUS.13, VUS.14, WHII.14 Mathematics: A.3, A.4, A.5
60	Describe types of cyber threats.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: GOVT.12, GOVT.16, VUS.13, VUS.14, WHII.14
61	Analyze types of current cyber threats.	History and Social Science: GOVT.12, GOVT.16, VUS.13, VUS.14, WHII.14
62	Identify the perpetrators of different types of malicious hacking.	
63	Describe the characteristics of vulnerabilities.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5 History and Social Science: GOVT.16, VUS.13, VUS.14

		Mathematics: COM.1, COM.2, COM.18
64	Identify the prevention of and protections against cyber threats.	
65	Identify the cyber risks associated with bring your own device (BYOD) opportunities on computer networks.	History and Social Science: VUS.13, VUS.14
66	Differentiate between ethics and laws.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: GOVT.16
67	Distinguish among types of ethical concerns.	History and Social Science: GOVT.16
68	Define *cyber bullying*.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5 History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14
69	Identify actions that constitute cyber bullying.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14
70	Identify possible warning signs of someone being cyber bullied.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: GOVT.16
71	Identify laws applicable to cybersecurity.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: GOVT.9, VUS.13, VUS.14, WHII.14
72	Explain the concept of "personally identifiable information."	English: 9.3, 9.5, 9.6, 9.8, 10.8, 11.3, 11.5, 11.6, 11.8, 12.5, 12.6, 12.8 History and Social Science: VUS.6, VUS.13, VUS.14, WHII.14 Mathematics: COM.1, PS.1*

73	Explain how and why personal data is valuable to both an individual and to the organizations (e.g., governments, businesses) that collect it, analyze it, and make decisions based on it.	English: 9.3, 9.5, 9.8, 10.3, 10.5, 10.8, 11.3, 11.5, 11.8, 12.3, 12.5, 12.8 History and Social Science: VUS.13, VUS.14, WHII.14 Mathematics: COM.1, PS.1*
74	Identify ways to control and protect personal data.	English: 9.5, 9.8, 10.5, 10.8, 11.5, 11.8, 12.5, 12.8 History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14 Mathematics: COM.1
75	Demonstrate net etiquette (*netiquette*) as it relates to cybersecurity.	History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14
76	Analyze the social and legal significance of the ongoing collection of personal digital information.	English: 9.5, 9.6, 9.8, 10.5, 10.6, 10.8, 11.5, 11.6, 11.8, 12.5, 12.6, 12.8 History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14
77	Distinguish between data, information, and knowledge.	English: 9.3, 10.3, 11.3, 12.3 Mathematics: COM.1, PS.1*
78	Identify the most common ways data is collected.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5 Mathematics: PS.8*
79	Identify the most common ways data can be stored.	History and Social Science: VUS.13, VUS.14 Mathematics: COM.16
80	Explain the difference between data at rest, data in transit, and data being processed.	English: 9.3, 10.3, 11.3, 12.3 Mathematics: COM.16

81	Identify the most common ways data is used.	English: 9.5, 10.5, 11.5, 12.5 Mathematics: COM.11
82	Discuss how data can be compromised, corrupted, or lost.	English: 9.5, 10.5, 11.5, 12.5 Mathematics: COM.10, COM.11, COM.16
83	Explain how businesses and individuals can protect themselves against threats to their data (e.g., firewalls, encryption, disabling, backups, permissions).	English: 9.5, 10.5, 11.5, 12.5 Mathematics: COM.16
84	Define the function of a computer operating system.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5 History and Social Science: VUS.1, VUS.14 Mathematics: COM.16, DM.8
85	Identify the components of an operating system.	History and Social Science: VUS.13, WHII.14
86	List types of operating systems.	History and Social Science: VUS.13, VUS.14, WHII.14
87	Evaluate the potential vulnerabilities, threats, and common exploits to an operating system.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: VUS.13, VUS.14, WHII.14
88	Identify best practices for protecting operating systems.	
89	Describe the concept of malware and techniques to guard against it.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: VUS.13
90	Evaluate critical operating system security parameters.	
91	Describe security and auditing logs.	English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5
92	Describe the role of a system backup.	English: 9.5, 10.5, 11.5, 12.5 Mathematics: COM.1
93	Define *virtualization technology*.	English: 9.3, 10.3, 11.3, 12.3

94	Identify advantages and disadvantages of using virtual machines.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: VUS.13, VUS.14, WHII.14 Mathematics: A.9, AII.9, AII.10
95	Define *programming* in the context of cybersecurity.	English: 9.3, 10.3, 11.3, 12.3 History and Social Science: VUS.13, VUS.14, WHII.14 Mathematics: COM.1
96	Differentiate between computer programming languages.	
97	Evaluate common programming flaws that lead to vulnerabilities.	History and Social Science: VUS.13, VUS.14, WHII.14 Mathematics: COM.1, COM.2
98	Identify best practices in secure coding and design.	Mathematics: COM.10
99	Identify ubiquitous computing.	History and Social Science: VUS.13, VUS.14, WHII.14
100	Discuss security and privacy implications of ubiquitous computing.	English: 9.5, 10.5, 11.5, 12.5 History and Social Science: VUS.13, VUS.14, WHII.14
101	Research career opportunities for cybersecurity professionals.	English: 9.8, 10.8, 11.8, 12.8 History and Social Science: GOVT.1, GOVT.15
102	Explore the Career Clusters affected by current and emerging technology.	English: 9.8, 10.8, 11.8, 12.8 History and Social Science: GOVT.16, VUS.13, VUS.14, WHII.14
103	Identify the educational pathways for emerging cybersecurity professionals.	English: 9.5, 9.8, 10.5, 10.8, 11.5, 11.8, 12.5, 12.8 History and Social Science: GOVT.1

104	Identify career paths and job titles within the cybersecurity/cyber forensics industry and Career Clusters.	English: 9.5, 9.8, 10.5, 10.8, 11.5, 11.8, 12.5, 12.8 History and Social Science: VUS.14
105	Research the cyber threats and security measures related to career pathways.	English: 9.8, 10.8, 11.8, 12.8 History and Social Science: VUS.14 Mathematics: COM.16
106	Identify testing skills/strategies for a certification examination.	
107	Describe the process and requirements for obtaining industry certifications related to the Cybersecurity Fundamentals course.	English: 9.5, 9.8, 10.5, 10.8, 11.5, 11.8, 12.5, 12.8
108	Demonstrate the ability to complete selected practice examinations (e.g., practice questions similar to those on certification exams).	
109	Successfully complete an industry certification examination representative of skills learned in this course (e.g., Microsoft, IC3, CompTIA).	History and Social Science: VUS.14

Teacher Resources

The Academic Initiative of the Cyber Innovation Center offers access to its curricula at no cost to K-12 teachers. These lessons could be used to supplement the following tasks:

- Task 40: Describe cybersecurity threats to an organization. (How Businesses Secure Information)
- Task 43: Describe the cyberattack surface of various organizations (How Businesses Secure Information)
- Task 64: Distinguish among types of ethical concerns. (Privacy vs. Security)
- Task 73: Explain the concept of "personally identifiable information." (You are the Data)
- Task 74: Explain how and why personal data is valuable to both an individual and to the organizations. (You are the Data)
- Task 75: Identify ways to control and protect personal data. (You are the Data)
- Task 77: Analyze the social and legal significance of the ongoing collection of personal digital information. (Your Permanent Electronic Record)

The National Institute of Standards and Technology has published the *Glossary of Key Information Security Terms*, which has been extracted from federal standards, publications, reports, and instructions.

The SANS Institute offers free professional development curricula focused on the fundamentals of cybersecurity. The course covers operating systems, networking, and systems administration.

The Virginia Cyber Range is a Commonwealth of Virginia initiative with a mission to enhance cybersecurity education for students in the Commonwealth's public high schools, colleges, and universities. The Virginia Cyber Range seeks to increase the number of fully prepared students entering the cybersecurity workforce in operations, development, and research. The Virginia Cyber Range provides an extensive Courseware Repository for educators and a cloud-hosted Exercise Area environment for hands-on cybersecurity labs and exercises for students.

AFA CyberPatriot the National Youth Cyber Education Program created by the Air Force Association to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future. At the core of the program is the National Youth Cyber Defense Competition, the nation's largest cyber defense competition that puts high school and middle school students in charge of securing virtual networks.

Net Etiquette

"What do I need to know about technology?" Northern Virginia Community College

"Netiquette," Justice Institute of British Columbia

Coding Standards

"SEI CERT Coding Standards," Software Engineering Institute, Carnegie-Mellon University

Open Web Application Security Project (OWASP), focused on improving the security of software.

Job-related Tools and Data

CyberSeek: Provides detailed data about supply and demand in cybersecurity fields, including an interactive state-by-state map which shows the field where demand is highest. For job seekers, educators, school counselors, and students.

Burning Glass Technologies: Job market analytics firm which looks at trends in hiring. Includes research about the cybersecurity job market.

"Breaking the Code on a Career in Cybersecurity": Virginia Space Grant Consortium's free video series, which features interviews with cyber professionals about their career pathways.

Highly Ranked Cybersecurity Programs: CNA, a nonprofit research and analysis organization, has created a tool to filter and sort cybersecurity programs in each state.

Microsoft Imagine Academy Resources

Microsoft Imagine Academy (MSIA) offers classroom resources and materials and instructional techniques that will help enhance instruction and learning for this course. Using the school's membership ID and product key for the Microsoft Imagine Academy, all resources are available through the MSIA Member Dashboard on the Microsoft site.

- To access the curriculum resources, select the Classroom Tile from the member site.
- To access downloadable curriculum resources including the MOAC e-Book, Lesson Plans, and Study Guides select Curriculum Overview - Curriculum Downloads.
- To access Online Learning videos and tutorials select Online Learning Directory tile.
- For more information visit: How to Get Started with Microsoft Imagine Academy Program.

Appendix: Credentials, Course Sequences, and Career Cluster Information

Industry Credentials: Only apply to 36-week courses

- Apple Certified Support Professional Examination
- Certified Associate in Python Programming (PCAP) Examination
- Certified Entry-Level Python Programmer (PCEP) Examination
- Cloud Essentials Certification Examination
- Cyber Forensics Associate Examination
- Ethical Hacking Associate Examination
- IC3 Digital Literacy Certification Examination
- IT Fundamentals+ Certification Examination
- Microsoft Technology Associate (MTA) Examinations
- Security Pro Certification Examination
- Security+ Certification Examination
- Workplace Readiness Skills for the Commonwealth Examination

Concentration sequences: *A combination of this course and those below, equivalent to two 36-week courses, is a concentration sequence. Students wishing to complete a specialization may take additional courses based on their career pathways. A program completer is a student who has met the requirements for a CTE concentration sequence and all other requirements for high school graduation or an approved alternative education program.*

- Cybersecurity in Family and Consumer Sciences (8291/36 weeks)
- Cybersecurity in Family and Consumer Sciences, Advanced (8292/36 weeks)
- Cybersecurity in Food and Agriculture (8074/36 weeks)
- Cybersecurity in Food and Agriculture, Advanced (8075/36 weeks)
- Cybersecurity in Manufacturing (8499/36 weeks)
- Cybersecurity in Manufacturing, Advanced (8496/36 weeks)
- Cybersecurity in Marketing (8126/36 weeks)
- Cybersecurity in Marketing, Advanced (8127/36 weeks)
- Cybersecurity Software Operations (6304/36 weeks)
- Cybersecurity Software Operations, Advanced (6306/36 weeks)
- Cybersecurity Systems Technology (8628/36 weeks, 140 hours)
- Health Informatics (8338/36 weeks)
- Healthcare Information Security (8339/36 weeks)

Career Cluster: Government and Public Administration	
Pathway	**Occupations**
National Security	**Military Intelligence Specialist**
Planning	**Interviewer**
Public Management and Administration	**Government Accountant/Auditor**
Regulation	**Cyber Crime Investigator** **Financial Analyst** **Privacy Compliance Manager**

Career Cluster: Government and Public Administration	
Pathway	**Occupations**
Revenue and Taxation	**Financial Analyst**

Career Cluster: Information Technology	
Pathway	**Occupations**
Information Support and Services	**Computer Support Specialist** **Database Administrator** **Database Analyst** **Information Systems Analyst** **Internet Entrepreneur** **Network Systems and Data Communication Analyst** **Software Test Engineer** **Systems Analyst**
Network Systems	**Computer Security Specialist** **Computer Systems Engineer, Architect** **Database Analyst** **Information Security Analyst** **Network and Computer Systems Administrator** **Network Architect** **Network Systems and Data Communication Analyst** **Systems Analyst**
Programming and Software Development	**Applications Integrator** **Computer Software Engineer** **Game Designer, Programmer** **Informatics Nurse Specialists** **Information Security Analyst** **Multimedia Artist, Animator** **Network Systems and Data Communication Analyst** **Programmer** **Project Manager** **Software Applications Engineer** **Software Test Engineer** **Systems Analyst** **Web Developer**
Web and Digital Communications	**Applications Integrator** **Computer Support Specialist** **Computer Systems Engineer, Architect** **Game Designer, Programmer** **Project Manager** **Software Test Engineer** **Systems Analyst** **Web Developer**

Career Cluster: Law, Public Safety, Corrections and Security	
Pathway	**Occupations**
Law Enforcement Services	**Private Detective, Investigator**
Legal Services	**Cyber Legal Advisor**

Career Cluster: Law, Public Safety, Corrections and Security	
Pathway	**Occupations**
Security and Protective Services	**Private Detective, Investigator**

Career Cluster: Science, Technology, Engineering and Mathematics	
Pathway	**Occupations**
Engineering and Technology	**Computer Programmer** **Computer Software Engineer**
Science and Mathematics	**Bioinformatics Technician**