Cybersecurity Fundamentals

6302/36 weeks

Table of Contents

Acknowledgments ......................................................................................................................................... 1
Course Description ........................................................................................................................................ 2
Task Essentials Table .................................................................................................................................... 2
Curriculum Framework ................................................................................................................................. 4
Understanding Cyber Threats and Vulnerabilities ...................................................................................... 16
Exploring Ethics as it Relates to Cybersecurity .......................................................................................... 23
Exploring Data Privacy .................................................................................................................................. 27
Examining Data Security as it Relates to Cybersecurity .......................................................................... 30
Programming as a Component of Cybersecurity ....................................................................................... 40
Exploring Cybersecurity Implications for Current and Emerging Technologies ................................. 43
Exploring Cybersecurity Careers ................................................................................................................ 44
Preparing for Industry Certification ............................................................................................................. 47
SOL Correlation by Task ............................................................................................................................... 49
Teacher Resources ...................................................................................................................................... 53
Appendix: Credentials, Course Sequences, and Career Cluster Information ............................................. 62

Acknowledgments

The components of this instructional framework were developed by the following curriculum development panelists:

- Julie Back, STEM Education Program Specialist, Department of Educational Foundations and Leadership, Old Dominion University
- Diana Bohuslov, Instructor, Battlefield High School, Prince William County Public Schools
- Dr. Darrell Carpenter, Director, Center for Cyber Security, Longwood University, Longwood
- Ernest Compton, Instructor, Pulaski County High School, Pulaski County Public Schools
- Dr. Charles Gardner, Director of Curriculum, CYBER.ORG, Bossier City, LA
- Christopher Long, Instructor, South County High School, Fairfax County Public Schools
- Jennifer Marden, Instructor, Loudoun County High School, Loudoun County Public Schools
- Dr. David Raymond, Director, Virginia Cyber Range, Virginia Tech
- Kristi Rice, Instructor, Spotsylvania High School, Spotsylvania County Public Schools
- Katrina Rigglemann, Instructor, Riverbend High School, Spotsylvania County Public Schools
- Shawn Thomas, Security Manager, Verizon Media, Ashburn

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

- Leslie R. Bowers, English Teacher (ret.), Newport News Public Schools
- Vickie L. Inge, Mathematics Committee Member, Virginia Mathematics and Science Coalition
- Anne F. Markwith, New Teacher Mentor (Science), Gloucester County Public Schools
- Michael L. Nagy, Social Studies Department Chair, Rustburg High School, Campbell County Public Schools
The framework was edited and produced by the CTE Resource Center:

- Leanne Forbes Tipton, Writer/Editor
- Kevin P. Reilly, Administrative Coordinator

Virginia Department of Education Staff

Judith Sams, Specialist, Business and Information Technology Education and Related Clusters
Dr. J. Anthony Williams, Curriculum and Instruction Coordinator
Dr. David S. Eshelman, Director, Workforce Development and Initiatives
George R. Willcox, Director, Operations and Accountability
Office of Career, Technical, and Adult Education
Virginia Department of Education

Copyright © 2021

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. Exciting opportunities will be presented to use interactive current resources in the study of cybersecurity such as Virginia Cyber Range, Virginia Space Grant Consortium, and Cyber.Org. Students will have the opportunity to prepare for success on related industry certifications aligned to the course content.

Task Essentials Table

- 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.

<table>
<thead>
<tr>
<th>Task Number</th>
<th>6302</th>
<th>Task/Competencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploring Cybersecurity Fundamentals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>+</td>
<td>Describe cybersecurity.</td>
</tr>
<tr>
<td>40</td>
<td>+</td>
<td>Describe the critical factors of information assurance.</td>
</tr>
<tr>
<td>41</td>
<td>+</td>
<td>Define vulnerability and risk.</td>
</tr>
<tr>
<td>42</td>
<td>+</td>
<td>Explain why organizations need to manage risk.</td>
</tr>
<tr>
<td>43</td>
<td>+</td>
<td>Identify the concepts of cybersecurity risk management.</td>
</tr>
<tr>
<td>44</td>
<td>+</td>
<td>Describe cybersecurity threats to an organization.</td>
</tr>
<tr>
<td>45</td>
<td>+</td>
<td>Describe national and industry standards and regulations that relate to cybersecurity.</td>
</tr>
<tr>
<td>46</td>
<td>+</td>
<td>Describe the cyberattack surface of various organizations.</td>
</tr>
<tr>
<td>47</td>
<td>+</td>
<td>Analyze risks affecting critical infrastructure.</td>
</tr>
<tr>
<td>Examining Computer Networks as a Foundational Element of Cybersecurity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>+</td>
<td>Describe computer components.</td>
</tr>
<tr>
<td>49</td>
<td>+</td>
<td>Describe a network.</td>
</tr>
<tr>
<td>50</td>
<td>+</td>
<td>Describe a wired network.</td>
</tr>
<tr>
<td>51</td>
<td>+</td>
<td>Describe a wireless network.</td>
</tr>
<tr>
<td>52</td>
<td>○</td>
<td>Compare wired and wireless networks.</td>
</tr>
<tr>
<td>53</td>
<td>+</td>
<td>Compare networking conceptual models.</td>
</tr>
<tr>
<td>54</td>
<td>+</td>
<td>Discuss services and potential vulnerabilities.</td>
</tr>
<tr>
<td>Number</td>
<td>Task</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>Differentiate between network types.</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>Describe the concept of the Internet as a network of connected systems.</td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>Identify networking protocols.</td>
<td></td>
</tr>
<tr>
<td><strong>Understanding Cyber Threats and Vulnerabilities</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>Differentiate between a cyber threat and a vulnerability.</td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>Describe types of cyber threats.</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>Analyze types of current cyber threats.</td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>Describe the concept of malware and the techniques to guard against it.</td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>Identify the perpetrators of different types of malicious hacking.</td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Describe the characteristics of vulnerabilities.</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>Identify the prevention of and protections against cyber threats.</td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>Identify the cyber risks associated with bring your own device (BYOD) opportunities on computer networks.</td>
<td></td>
</tr>
<tr>
<td><strong>Exploring Ethics as it Relates to Cybersecurity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>Differentiate between ethics and laws.</td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>Distinguish among types of ethical concerns.</td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>Define cyberbullying.</td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>Identify actions that constitute cyberbullying.</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>Identify possible warning signs of someone being cyberbullied.</td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>Demonstrate net etiquette (i.e., netiquette) as it relates to cybersecurity.</td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>Identify laws applicable to cybersecurity.</td>
<td></td>
</tr>
<tr>
<td><strong>Exploring Data Privacy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>Explain the concept of “personally identifiable information.”</td>
<td></td>
</tr>
<tr>
<td>74</td>
<td>Explain why personal data is valuable to both an individual and to organizations (e.g., governments, businesses) that collect it, analyze it, and make decisions based on it.</td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>Explain the techniques used to collect personal data through social media, web tracking, and mobile devices.</td>
<td></td>
</tr>
<tr>
<td>76</td>
<td>Identify ways to control and protect personal data.</td>
<td></td>
</tr>
<tr>
<td>77</td>
<td>Analyze the social and legal significance of the ongoing collection of personal digital information.</td>
<td></td>
</tr>
<tr>
<td><strong>Examining Data Security as it Relates to Cybersecurity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>Distinguish between data, information, and knowledge.</td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>Identify the most common ways data is collected.</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>Identify the most common ways data can be stored.</td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>Explain the difference between data at rest, data in transit, and data being processed.</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>Identify the most common ways data is used.</td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>Discuss how data can be compromised, corrupted, or lost.</td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>Explain how businesses and individuals can protect themselves against threats to their data.</td>
<td></td>
</tr>
<tr>
<td><strong>Securing Operating Systems</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>85</td>
<td>Define the function of a computer operating system.</td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>Identify the components of an operating system.</td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>List types of operating systems.</td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>Identify examples of widely used desktop and server operating systems.</td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>Evaluate the potential vulnerabilities, threats, and common exploits to an operating system.</td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>Identify best practices for protecting operating systems.</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>Evaluate critical operating system security parameters.</td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>Describe security and auditing logs.</td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>Describe the role of a system backup.</td>
<td></td>
</tr>
<tr>
<td>94</td>
<td>Define virtualization technology.</td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>Identify advantages and disadvantages of using virtual machines.</td>
<td></td>
</tr>
</tbody>
</table>
Curriculum Framework

Exploring Cybersecurity Fundamentals

Task Number 39

Describe cybersecurity.

Definition

Description should state that cybersecurity is the protection of information and data from risks associated with threats, attacks, hazards, or physical damage. Risks may include, but are not limited to:

- information systems (e.g., networks, hardware, software)
- the human element
- physical elements

from risks associated with threats, attacks, hazards, or physical damage.

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills

Cyber Security

Healthcare Administration

Introduction to Information Technology
Task Number 40
Describe the critical factors of information assurance.

Definition
Description should include

- explaining that the Central Intelligence Agency (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 goals within the CIA triad and defining the terms as they apply to cybersecurity
  - confidentiality—ensures that data are only accessed by authorized person(s) through security measures such as usernames and passwords and access control lists (ACL)
  - integrity—ensures the data are trusted. This means data must be guarded against unauthorized changes; methods of ensuring integrity include data permissions and encryption
  - availability—provides 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

- authentication—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
Business Knowledge and Skills
Business Ethics
Business Law
Cyber Security
Healthcare Administration
Introduction to Information Technology
Network Design
Networking Infrastructure

Task Number 41
Define vulnerability and risk.

Definition
Definition should state that
• **vulnerability** refers to a flaw in a system that can leave it open to attack; may also refer to any type of weakness in a computer system, in a set of procedures, or in anything that leaves information security exposed to a threat.*
• **risk** is the likelihood that a vulnerability will occur and that a loss occurs if that vulnerability is exploited.

*Technopedia ([www.techopedia.com/definition/13484/vulnerability](http://www.techopedia.com/definition/13484/vulnerability)).

### FBLA Competitive Events and Activities Areas

- Business Knowledge and Skills
- Business Ethics
- Business Law
- Cyber Security
- E-business
- Healthcare Administration
- Introduction to Information Technology
- Management Decision Making
- Management Information Systems
- Network Design
- Networking Infrastructure
- Website Design

---

### Task Number 42

**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 effects of those threats.

Because all threats cannot be completely eliminated, organizations must address responses to threats and plans for continuous business operations.

### FBLA Competitive Events and Activities Areas

- Business Knowledge and Skills
- Business Ethics
- Business Law
- Cyber Security
- Healthcare Administration
- Introduction to Information Technology
- Management Decision Making
- Management Information Systems
- Network Design
**Task Number 43**

**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 an organization’s exposure to 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., a retailer discontinues personal data collection of customers to avoid the risk that the data could be stolen)
  - *risk acceptance*—understanding and accepting the risks associated with use of a system or feature; this often happens when the cost of mitigation outstrips the potential loss associated with the risk.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Ethics

Business Law

Cyber Security

E-business

Healthcare Administration

Introduction to Information Technology

Management Decision Making

Management Information Systems

Network Design

Networking Infrastructure

Website Design

---

**Task Number 44**

**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
  - email
  - social engineering
  - insider threats
  - network threats
physical threats such as fire or floods
threats stemming from software systems or user actions.

Teacher resource:

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Business Law
Cyber Security
E-business
Healthcare Administration
Introduction to Information Technology
Management Decision Making
Management Information Systems
Network Design
Networking Infrastructure
Website Design

Task Number 45
Describe national and industry standards and regulations that relate to cybersecurity.

Definition
Description should include, but not be limited to, the following:

- Standards and regulations are determined based on the data each stores.
- Standards—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.
- Regulations—requirements by a government agency that must be followed. For example, in the healthcare 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).

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Business Law
Cyber Security
E-business
Healthcare Administration
Task Number 46  
Describe the cyberattack surface of various organizations.  

**Definition**  
Description should include a definition of threat modeling and 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:**  
CYBER.ORG [Cyber Business Module: How Businesses Secure Information](https://cyber.org/cyber-society/business)

**FBLA Competitive Events and Activities Areas**  
Business Knowledge and Skills  
Business Ethics  
Business Law  
Cyber Security  
E-business  
Healthcare Administration  
Introduction to Information Technology  
Management Decision Making  
Management Information Systems  
Network Design  
Networking Infrastructure  
Website Design

---

Task Number 47  
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 Cybersecurity and Infrastructure Security Agency (CISA) 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.

Teacher resource:

Critical Infrastructure Sectors, Cybersecurity and Infrastructure Security Agency (https://www.cisa.gov/critical-infrastructure-sectors)

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills
Business Ethics
Business Law
Cyber Security
E-business
Healthcare Administration
Hospitality and Event Management
Introduction to Information Technology
Management Decision Making
Management Information Systems
Network Design
Networking Infrastructure
Sports and Entertainment Management
Website Design

---

Examining Computer Networks as a Foundational Element of Cybersecurity

Task Number 48

Describe computer components.

Definition

Description should include
• case
• motherboard
• central processing unit (CPU)
• random access memory (RAM)
• hard drive
• power supply
• ports.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Computer Problem Solving
Introduction to Information Technology

Task Number 49
Describe a network.

Definition
Description should include identifying

• the purpose of a network
• the physical components of a network, including, but not limited to
  o network interface card (NIC)
  o switch
  o router
  o wireless access point
• software components of a network, including, but not limited to
  o operating systems
  o network operating systems or network operations and management
  o firewalls
  o network security applications.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Computer Problem Solving
Cyber Security
Introduction to Information Technology
Network Design
Networking Infrastructure

Task Number 50
Describe a wired network.

Definition
Description should include
• defining *wired network* as a network in which all components are connected with fiber optic cables; 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 the Institute of Electrical and Electronics Engineers (IEEE) 802 standards and recommended practices, particularly 802.1 and 802.3.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills
Computer Problem Solving
Cyber Security
Introduction to Information Technology
Network Design
Networking Infrastructure

---

**Task Number 51**

**Describe a wireless network.**

**Definition**

Description should include

• defining *wireless network* as a computer network in which connections are made without computer cables.
• Explaining the basis of wireless transmissions is radio waves (e.g., radio waves connect devices to the Internet and to a business network and its applications)
• explaining 802.11 wireless local area network standards
• explaining authentication types.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills
Computer Problem Solving
Cyber Security
Introduction to Information Technology
Network Design
Networking Infrastructure

---

**Task Number 52**

**Compare wired and wireless networks.**

**Definition**

Comparison should include

• the cost of a network installation
• the cost to operate and maintain a network
• network speed
• network reliability
• network security.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Computer Problem Solving
Cyber Security
Introduction to Information Technology
Network Design
Networking Infrastructure

Task Number 53
Compare networking conceptual models.

Definition
Comparison should include the following models:

• Open Systems Interconnect (OSI)—seven-layer model that describes communication between systems. The layers are as follows:
  o Application
  o Presentation
  o Session
  o Transport
  o Network
  o Data link
  o Physical

• Internet (Transmission Control Protocol [TCP]/Internet Protocol [IP])—a four-layer model that describes communication between systems. The layers are as follows:
  o Application
  o Transport
  o Internet
  o Network

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Computer Problem Solving
Cyber Security
Introduction to Information Technology
Network Design
Networking Infrastructure

Task Number 54
Discuss services 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
  - http services
  - wireless sensor network.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Computer Applications

Computer Problem Solving

Cyber Security

Database Design and Application

Introduction to Information Technology

Network Design

Networking Infrastructure

Spreadsheet Applications

Word Processing

---

**Task Number 55**

**Differentiate between network types.**

**Definition**

Differentiation may include the following:

- Local Area Networks (LAN)—a collection of computers, peripherals, and other devices that communicate across a network (e.g., wire, fiber optic, wireless) in a single network segment; LANs differ from Wide Area Networks (WANs) in their reliance on local addressing schemes and their ability to operate without knowledge of neighboring networks.
  - LANs rely on local addressing and local network communications protocols (e.g., Address Resolution Protocol [ARP]) 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 use addressing schemes (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.
  - The Internet is the most widely known example of a wide area network.
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 Campus Area Network (CAN), Metropolitan Area Network (MAN), or Global Area Network (GAN).

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

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Computer Problem Solving
Cyber Security
Introduction to Information Technology
Network Design
Networking Infrastructure

Task Number 56
Describe the concept of the Internet as a network of connected systems.

Definition
Description should include

- a definition of the Internet as a global system of interconnected computer networks that use the Internet Protocol Suite (TCP/IP) to link billions of devices worldwide.
- the concept that 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
Business Knowledge and Skills
Computer Problem Solving
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructure

Task Number 57
Identify networking protocols.

Definition
Identification should include descriptions of
• application layers protocols
  o Hypertext Transfer Protocol (HTTP)—an application-layer protocol used primarily on the Internet to request and receive web content from servers to browsers; a stateless and connectionless protocol
  o 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
  o File Transfer Protocol (FTP)—a client/server protocol used for transferring files to or exchanging files with a host computer; FTP is widely used on the Internet for moving or transferring files from one computer to another
  o Post Office Protocol (POP)—a type of computer networking and Internet standard protocol retrieves and extracts email from a remote mail server for access by the host machine or portable device

• transport layer protocols
  o Transmission Control Protocol (TCP)—a transport layer communications protocol used to send network data between hosts; TCP is a connection-oriented protocol that provides reliable message transmission
  o User Datagram Protocol (UDP)—a transport layer communications protocol used to send network data between hosts; UDP is referred to as an unreliable protocol because it does not guarantee message delivery or in-order message reception

• Internet layer protocols
  o Internet Protocol (IP)—the primary network protocol by which data is sent from one computer to another; computers are identified on the internet using Internet Protocol addresses
  o Internet Control Message Protocol (ICMP)—a part of the Internet protocol suite used by network devices to send error messages and other operational information to other devices on the network
  o Dynamic Host Configuration Protocol (DHCP)—a local network protocol that automatically assigns Internet Protocol addresses to network hosts

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Computer Problem Solving
Cyber Security
E-business
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructure
Website Design

Understanding Cyber Threats and Vulnerabilities

Task Number 58
Differentiate between a cyber threat and a vulnerability.

**Definition**

Differentiation 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, technical failures)
- defining *vulnerability*
- explaining
  - how a vulnerability can result in a threat
  - how eliminating vulnerabilities can eliminate a threat
  - what exploits are
  - how to calculate risk.

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills
- Coding and Programming
- Computer Game & Simulation
- Computer Problem Solving
- Cyber Security
- Database Design and Application
- E-business
- Introduction to Information Technology
- Management Information Systems
- Network Design
- Networking Infrastructure
- Website Design

---

**Task Number 59**

**Describe types of cyber threats.**

**Definition**

Description should include, but not be limited to

- authentication (e.g., password attacks, biometrics attacks)
- social engineering, including phishing and other scams
- web application attacks such as injection attacks and scripting attacks
- exploitation of operating system and application software vulnerabilities
- malicious code and malware
- denial of service attacks
- 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 human immunodeficiency virus (HIV) and acquired immunodeficiency syndrome (AIDS), respiratory syndromes, Ebola virus disease, Marburg virus disease, Nipah virus (NiV) infection, and Zika virus. Several of
these have spread extensively in human populations to cause a global epidemic (i.e., 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**

*Business Knowledge and Skills*

*Coding and Programming*

*Computer Game & Simulation*

*Computer Problem Solving*

*Cyber Security*

*Database Design and Application*

*E-business*

*Introduction to Information Technology*

*Management Information Systems*

*Network Design*

*Networking Infrastructure*

*Website Design*

---

**Task Number 60**

**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.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Coding and Programming
Computer Game & Simulation
Computer Problem Solving
Cyber Security
Database Design and Application
E-business
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructure
Website Design

Task Number 61
Describe the concept of malware and the techniques to guard against it.

Definition
Description should include

• the types of malware and methods of propagation
• the role of antivirus and antispyware utilities
• the way to distinguish between available antivirus and antispyware utilities
• the types of current and emerging techniques.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Computer Problem Solving
Coding and Programming
Computer Game & Simulation Programming
Cyber Security
Database Design and Application
E-business
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructure
Website Design
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 advanced persistent threat (APT) hacking groups
- cyber warriors (i.e., members of a government agencies and military team of elite cybersecurity professionals).

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Computer Problem Solving
Coding and Programming
Computer Game & Simulation Programming
Cyber Security
Database Design and Application
E-business
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructure
Website Design

Task Number 63
Describe the characteristics of vulnerabilities.

Definition
Description should include

- defining the term vulnerability as a weakness that 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
  - 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
  o buffer overflow or broken authentication and session management
  o injection vulnerabilities
  o input validation
  o privilege confusion
• evaluating vulnerabilities as they relate to
  o physical facilities and the environment of the system or personnel working with the system
  o operational procedures, including security measures
  o business operations
  o hardware
  o software
  o communication equipment and network (individually or in combination)

Teacher resource:
• Common Vulnerabilities and Exposures, (https://cve.mitre.org/)

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Computer Problem Solving
Coding and Programming
Computer Game & Simulation Programming
Cyber Security
Database Design and Application
E-business
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructure
Website Design

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, firewalls, end point protection software, intrusion detection system [IDS]/intrusion prevention system [IPS], vulnerability scanners).
• 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.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Coding and Programming
Computer Game & Simulation Programming
Cyber Security
Database Design and Application
E-business
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructure
Website Design

Task Number 65
Identify the cyber risks associated with bring your own device (BYOD) opportunities on computer networks.

Definition
Identification should include how BYOD practices can expose a network to malware and other threats, creating additional vulnerabilities in a number of ways, such as

• Organizational controls such as password complexity and restrictions on software installation can be bypassed.
• Operating systems and software on devices used under a BYOD policy may not be patched and updated regularly.
• BYOD policies may not allow devices to run antivirus or other security software that are required for organization-owned devices.
• BYOD policy approved devices can download and store sensitive organizational data. Loss, theft, or other data compromises on these devices may not be reported.
• Personal devices and portable media can contain malware and could threaten the network or infect other systems if they are allowed to connect to an organization's network.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Computer Problem Solving
Exploring Ethics as it Relates to Cybersecurity

Task Number 66
Differentiate between ethics and laws.

Definition
Differentiation should include

- ethics—the moral principles that guide a person’s conduct
- laws—the set of accepted rules and regulations created by appropriate authorities, such as national, state, or local governments.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Business Law

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.
Task Number 68
Define cyberbullying.

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

Task Number 69
Identify actions that constitute cyberbullying.

Definition
Identification should include

- sending content perceived as harmful by messaging, email, and/or social media
- spreading rumors via email or by posting on social networking sites
- posting embarrassing pictures, videos, websites, or fake profiles.
Task Number 70
Identify possible warning signs of someone being cyberbullied.

Definition
Identification could include signs such as

- avoiding 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 a regular basis
- becoming withdrawn from friends or family
- avoiding discussion of what they do or where they go online
- failing to attend school regularly
- requesting permission to leave school without a justifiable excuse
- exhibiting stress or stress-related disorders
- performing poorly in academics.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Business Ethics
Business Law
Cyber Security

Task Number 71
Demonstrate net etiquette (i.e., netiquette) as it relates to cybersecurity.

Definition
Demonstration should include

- declining to post anything you would not say in person
- acknowledging and adhering to different standards of netiquette for different places
- paying attention to the content (i.e., grammar, punctuation, spelling, accuracy, tone)
- checking facts for accuracy and continually updating online information
- not misrepresenting your identity or hiding behind anonymity
- 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
o respecting others’ privacy
o not abusing your power
o forgiving other people’s mistakes.

Teacher resources:

- *What Do I Need to Know about Technology?* Northern Virginia Community College (https://online.nvcc.edu/orientation/know-about-technology.htm)

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Communication

Business Ethics

Business Law

Business Procedures

Cyber Security

Introduction to Business Communication

Introduction to Social Media Strategies

Social Media Strategies

---

**Task Number 72**

**Identify laws applicable to cybersecurity.**

**Definition**

Identification should include, but not be limited to

- national laws, regulations, policies, and/or standards
  - Computer Fraud and Abuse Act of 1986 (CFAA)
  - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001
  - Homeland Security Act of 2002
  - Digital Millennium Copyright Act (DMCA) 1998
  - Privacy Act of 1974
  - Electronic Communications Privacy Act (ECPA) of 1986
  - Cyber Security Information Sharing Act (CISA) of 2015
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Telecommunications Act of 1996
  - Gramm-Leach-Bliley Act (GLBA) of 1999
  - Family Educational Rights and Privacy Act (FERPA) of 1974
  - Sarbanes-Oxley Act of 2002

- international laws and standards (e.g., European Union and Information Security Directive).

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Business Ethics
Exploring Data Privacy

Task Number 73
Explain the concept of “personally identifiable information.”

Definition
Explanation should include

- defining personal data, including data elements such as name, address, social security number, telephone number, email address
- 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:
CYBER.ORG Cyber Business Module: You are the Data, (https://cyber.org/cyber-society/business)

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Cyber Security
Database Design and Application
E-Business
Healthcare Administration
Introduction to Information Technology
Introduction to Social Media Strategies
Social Media Strategies
Spreadsheet Application
Website Design

Task Number 74
Explain why personal data is valuable to both an individual and to 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:**
CYBER.ORG Cyber Business Module: You are the Data, [https://cyber.org/cyber-society/business](https://cyber.org/cyber-society/business)

**FBLA Competitive Events and Activities Areas**
Business Knowledge and Skills
Cyber Security
Database Design and Application
E-Business
Healthcare Administration
Introduction to Information Technology
Introduction to Social Media Strategies
Social Media Strategies
Spreadsheet Application
Website Design

---

**Task Number 75**

**Explain the techniques used to collect personal data through social media, web tracking, and mobile devices.**

**Definition**
Explanation should include

- first- and third-party cookies
- device fingerprinting
- information gathered by social networking sites
- information collected through search engines
- information provided voluntarily in exchange for services or access to services.

**FBLA Competitive Events and Activities Areas**
Business Knowledge and Skills
Cyber Security
Database Design and Application
E-Business
Healthcare Administration
Introduction to Information Technology
Introduction to Social Media Strategies
Task Number 76
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
- understanding that many apps allow users to control settings related to the amount of data shared.

Teacher resource:

CYBER.ORG, Cyber Business Module: You are the Data, [https://cyber.org/cyber-society/business](https://cyber.org/cyber-society/business)


FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Cyber Security
Database Design and Application
E-Business
Healthcare Administration
Introduction to Information Technology
Introduction to Social Media Strategies
Mobile Application Development
Social Media Strategies
Spreadsheet Application
Website Design

Task Number 77
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:**
CYBER.ORG, [Cyber Law Module: Your Permanent Electronic Record](https://cyber.org/cyber-society/law)

---

**FBLA Competitive Events and Activities Areas**
Business Knowledge and Skills
Business Ethics
Business Law
Cyber Security
Database Design and Application
E-Business
Healthcare Administration
Introduction to Information Technology
Introduction to Social Media Strategies
Mobile Application Development
Social Media Strategies
Spreadsheet Application
Website Design

---

**Examining Data Security as it Relates to Cybersecurity**

---

**Task Number 78**
**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
Business Knowledge and Skills
Business Communications
Business Ethics
Business Law
Cyber Security
Introduction to Business Communication

Task Number 79
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
  o active vs. passive
  o informed consent vs. no consent
• describing the types of sources where data can be collected.

FBLA Competitive Events and Activities Areas
Business Skills and Knowledge
Business Communication
Cyber Security
Database Design and Application
E-business
Introduction to Business Communication
Mobile Application
Website Design

Task Number 80
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
• cloud storage.
Task Number 81

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

**Definition**

Explanation should include

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

**FBLA Competitive Events and Activities Areas**

Business Skills and Knowledge
Business Communication
Cyber Security
Database Design and Application
E-business
Introduction to Business Communication
Introduction to Information Technology
Management Information Systems
Mobile Application
Network Design
Networking Infrastructures
Spreadsheet Applications
Website Design
Task Number 82
Identify the most common ways data is used.

**Definition**
Identification should include how to extract specific information from stored data (e.g., data filtering; data queries including structured query language [SQL]; data mining; data analytics).

**FBLA Competitive Events and Activities Areas**
- Business Skills and Knowledge
- Business Communication
- Cyber Security
- Database Design and Application
- E-business
- Healthcare Administration
- Introduction to Business Communication
- Introduction to Information Technology
- Management Information Systems
- Mobile Application
- Network Design
- Networking Infrastructures
- Spreadsheet Application
- Website Design

Task Number 83
Discuss how data can be compromised, corrupted, or lost.

**Definition**
Discussion should include

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

**FBLA Competitive Events and Activities Areas**
- Business Skills and Knowledge
- Business Communication
- Cyber Security
- Database Design and Application
- E-business
- Healthcare Administration
Task Number 84

**Explain how businesses and individuals can protect themselves against threats to their data.**

**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**

Business Skills and Knowledge

Cyber Security

Database Design and Application

E-business

Healthcare Administration

Introduction to Information Technology

Management Information Systems

Mobile Application

Network Design

Networking Infrastructures

Spreadsheet Application

Website Design
Securing Operating Systems

Task Number 85
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 Skills and Knowledge
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 86
Identify the components of an operating system.

Definition
Identification should include

- kernel
- shell
- utilities
- file system
- process management, including services
- networking.

FBLA Competitive Events and Activities Areas
Business Skills and Knowledge
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures
Task Number 87
List types of operating systems.

Definition
Listing should include

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

FBLA Competitive Events and Activities Areas
Business Skills and Knowledge
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 88
Identify examples of widely used desktop and server operating systems.

Definition
Identification should include

- Windows desktop operating systems (e.g., Windows 10)
- Windows servers OS (e.g., Windows Server 2019)
- Apple operating systems (e.g., iOS, MacOS)
- Linux operating systems (e.g., Kali, Ubuntu, CentOS).

FBLA Competitive Events and Activities Areas
Business Skills and Knowledge
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 89
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.

**Task Number 90**
**Identify best practices for protecting operating systems.**

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

**Task Number 91**
**Evaluate critical operating system security parameters.**

**Definition**
Evaluation should include establishing or following

- authentication policy
- access control (i.e., rights and permissions)
- audit policy.
Task Number 92
Describe security and auditing logs.

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

FBLA Competitive Events and Activities Areas
Business Skills and Knowledge
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 93
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.

FBLA Competitive Events and Activities Areas
Business Skills and Knowledge
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 94
Define virtualization technology.

Definition
Definition should include, but not be limited to

- what constitutes 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
• the key properties of virtual machines
  o partitioning
  o isolation
  o encapsulation
  o hardware independence
• the advantages and disadvantages of virtualization technology
• examples of virtualization platforms
  o Hyper-V
  o VMware
  o virtual box
  o cloud computing.

FBLA Competitive Events and Activities Areas

Business Skills and Knowledge
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 95

Identify advantages and disadvantages of using virtual machines.

Definition

Identification of advantages should include, but not be limited to

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

Identification of disadvantages should include, but not be limited to

• efficiency
  o virtual machines are not as efficient in accessing hardware as a real machine
  o multiple virtual machines running on a host computer may introduce unstable performance to the host on each virtual machine and thus affect the other virtual machine’s application
• cost
software for virtual machines may cost more due to the expense of virtualization software

- additional software management tools may be required
  - compatibility (e.g., not all servers and applications are virtualization-friendly)
  - complex root-cause analysis.

**FBLA Competitive Events and Activities Areas**

- Business Skills and Knowledge
- Cyber Security
- Introduction to Information Technology
- Management Information Systems
- Network Design
- Networking Infrastructures

---

**Programming as a Component of Cybersecurity**

**Task Number 96**

**Identify representation of data at lowest levels.**

**Definition**

Identification should include

- recognizing binary data
- recognizing hexadecimal data, and its relationship to binary data
- recognizing the representation of data in other common numbering systems such as Octal and Base64.

**FBLA Competitive Events and Activities Areas**

- Business Skills and Knowledge
- Cyber Security
- Database Design and Application
- Introduction to Information Technology
- Management Information Systems
- Network Design
- Networking Infrastructures

---

**Task Number 97**

**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 Skills and Knowledge
Coding and Programming
Computer Game and Simulation Programming
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 98
Differentiate between computer programming languages.
Definition
Differentiation should include

• compiled languages
• interpreted languages (i.e., scripting)
• markup languages.

FBLA Competitive Events and Activities Areas
Business Skills and Knowledge
Coding and Programming
Computer Game and Simulation Programming
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 99
Describe Python.
Definition
Description should include

• using programming to walk through designated lessons
• creating a basic program
• explaining the basic functions of Python coding.
Task Number 100
Demonstrate Linux.

Definition
Demonstration should include
- using Linux commands
- using command line interface.

Teacher resource:
Virginia Cyber Range, (https://www.virginiacyberrange.org/)

FBLA Competitive Events and Activities Areas
Business Skills and Knowledge
Coding and Programming
Computer Game and Simulation Programming
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 101
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 Skills and Knowledge

Coding and Programming

Computer Game and Simulation Programming

Cyber Security

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures

---

**Task Number 102**

**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 Skills and Knowledge

Coding and Programming

Computer Game and Simulation Programming

Cyber Security

Introduction to Information Technology

Management Information Systems

Network Design

Networking Infrastructures

---

**Exploring Cybersecurity Implications for Current and Emerging Technologies**

---

**Task Number 103**
Identify ubiquitous computing.

Definition
Identification should include, but not be limited to

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

FBLA Competitive Events and Activities Areas
Business Skills and Knowledge
Coding and Programming
Computer Game and Simulation Programming
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Task Number 104
Description security and privacy implications of ubiquitous computing.

Definition
Description should include examples of security and privacy issues in ubiquitous computing, such as IoT in smart homes, autonomous and semi-autonomous vehicles, and industrial control systems.

FBLA Competitive Events and Activities Areas
Business Skills and Knowledge
Coding and Programming
Computer Game and Simulation Programming
Cyber Security
Introduction to Information Technology
Management Information Systems
Network Design
Networking Infrastructures

Exploring Cybersecurity Careers

Task Number 105
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.

Teacher resource:
Breaking the Code on a Career in Cybersecurity, Virginia Space Grant Consortium (https://www.virginiacyberrange.org/)

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Introduction to Information Technology
Job Interview

Task Number 106
Examine the Career Clusters affected by current and emerging technology.

Definition
Examination 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
- Energy
- 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 Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Introduction to Information Technology
Task Number 107
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, Bureau of Labor Statistics’ Occupational Outlook Handbook, Virginia Education Wizard, CyberSeek, CNA’s Highly Ranked Cybersecurity Programs)
- 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 Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Introduction to Information Technology
Job Interview

Task Number 108
Identify career paths and job titles within the cybersecurity and/or 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 defender, cyber sleuth, information security analyst, network administrator, cybersecurity researcher, chief information security officer).

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Introduction to Information Technology
Task Number 109
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, popups)
- spam.

FBLA Competitive Events and Activities Areas
Business Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Introduction to Information Technology
Job Interview

Preparing for Industry Certification

Task Number 110
Identify testing skills and 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 Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Introduction to Information Technology
Job Interview

Task Number 111
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 and requirements for obtaining the certifications from official websites of the testing organization or 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.

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Introduction to Information Technology
Job Interview

Task Number 112

Demonstrate the ability to complete selected practice examinations.

Definition

Demonstration should include obtaining and successfully completing practice examinations for selected certifications related to the course (e.g., practice questions similar to those on certification exams). Practice examinations may be obtained from provider sites and/or materials from publishers.

FBLA Competitive Events and Activities Areas

Business Knowledge and Skills
Cyber Security
Electronic Career Portfolio
Introduction to Information Technology
Job Interview

Task Number 113

Successfully complete an industry certification examination representative of skills learned in this course.

Definition

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 (e.g., Microsoft Technology Associate, CompTIA).

**FBLA Competitive Events and Activities Areas**

Business Knowledge and Skills

Cyber Security

Electronic Career Portfolio

Introduction to Information Technology

Job Interview

---

**SOL Correlation by Task**

<table>
<thead>
<tr>
<th>Task Description</th>
<th>English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5</th>
<th>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe cybersecurity.</td>
<td>English: 9.5, 10.5, 11.5, 12.5</td>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Describe the critical factors of information assurance</td>
<td>English: 9.5, 10.5, 11.5, 12.5</td>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Define vulnerability and risk.</td>
<td>English: 9.5, 10.5, 11.5, 12.5</td>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Explain why organizations need to manage risk.</td>
<td>English: 9.5, 10.5, 11.5, 12.5</td>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Identify the concepts of cybersecurity risk management.</td>
<td>English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5</td>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Describe cybersecurity threats to an organization.</td>
<td>English: 9.5, 10.5, 11.5, 12.5</td>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Describe national and industry standards and regulations that relate to cybersecurity.</td>
<td>English: 9.5, 10.5, 11.5, 12.5</td>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Describe the cyberattack surface of various organizations.</td>
<td>English: 9.5, 10.5, 11.5, 12.5</td>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Analyze risks affecting critical infrastructure.</td>
<td>English: 9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5</td>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Describe computer components.</td>
<td>English: 9.5, 10.5, 11.5, 12.5</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Describe a network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Describe a wired network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Describe a wireless network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compare wired and wireless networks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compare networking conceptual models.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discuss services and potential vulnerabilities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Differentiate between network types.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Describe the concept of the Internet as a network of connected systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify networking protocols.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Differentiate between a cyber threat and a vulnerability.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Describe types of cyber threats.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze types of current cyber threats.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Describe the concept of malware and the techniques to guard against it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify the perpetrators of different types of malicious hacking.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Describe the characteristics of vulnerabilities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify the prevention of and protections against cyber threats.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify the cyber risks associated with bring your own device (BYOD) opportunities on computer networks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Differentiate between ethics and laws.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distinguish among types of ethical concerns.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define cyberbullying.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>English:</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5, 10.5, 11.5, 12.5</td>
</tr>
<tr>
<td>9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5</td>
</tr>
<tr>
<td>9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5</td>
</tr>
<tr>
<td>9.5, 10.5, 11.5, 12.5</td>
</tr>
<tr>
<td>9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5</td>
</tr>
<tr>
<td>9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5</td>
</tr>
<tr>
<td>9.5, 10.5, 11.5, 12.5</td>
</tr>
<tr>
<td>9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5</td>
</tr>
<tr>
<td>9.3, 9.5, 10.3, 10.5, 11.3, 11.5, 12.3, 12.5</td>
</tr>
<tr>
<td>9.5, 10.5, 11.5, 12.5</td>
</tr>
<tr>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Social Studies: WG 17; WHII 14; VUS 14; Govt 7, 8, 9, 12, 15</td>
</tr>
<tr>
<td>Identify actions that constitute cyberbullying.</td>
</tr>
<tr>
<td>Identify possible warning signs of someone being cyberbullied.</td>
</tr>
<tr>
<td>Demonstrate net etiquette (i.e., <em>netiquette</em>) as it relates to cybersecurity.</td>
</tr>
<tr>
<td>Identify laws applicable to cybersecurity.</td>
</tr>
<tr>
<td>Explain the concept of “personally identifiable information.”</td>
</tr>
<tr>
<td>Explain why personal data is valuable to both an individual and to organizations (e.g., governments, businesses) that collect it, analyze it, and make decisions based on it.</td>
</tr>
<tr>
<td>Explain the techniques used to collect personal data through social media, web tracking, and mobile devices.</td>
</tr>
<tr>
<td>Identify ways to control and protect personal data.</td>
</tr>
<tr>
<td>Analyze the social and legal significance of the ongoing collection of personal digital information.</td>
</tr>
<tr>
<td>Distinguish between data, information, and knowledge.</td>
</tr>
<tr>
<td>Identify the most common ways data is collected.</td>
</tr>
<tr>
<td>Identify the most common ways data can be stored.</td>
</tr>
<tr>
<td>Explain the difference between data at rest, data in transit, and data being processed.</td>
</tr>
<tr>
<td>Identify the most common ways data is used.</td>
</tr>
<tr>
<td>Discuss how data can be compromised, corrupted, or lost.</td>
</tr>
<tr>
<td>Explain how businesses and individuals can protect themselves against threats to their data.</td>
</tr>
<tr>
<td>Define the function of a computer operating system.</td>
</tr>
<tr>
<td>Identify the components of an operating system.</td>
</tr>
<tr>
<td>List types of operating systems.</td>
</tr>
<tr>
<td>Task</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>Identify examples of widely used desktop and server operating systems.</td>
</tr>
<tr>
<td>Evaluate the potential vulnerabilities, threats, and common exploits to an operating system.</td>
</tr>
<tr>
<td>Identify best practices for protecting operating systems.</td>
</tr>
<tr>
<td>Evaluate critical operating system security parameters.</td>
</tr>
<tr>
<td>Describe security and auditing logs.</td>
</tr>
<tr>
<td>Describe the role of a system backup.</td>
</tr>
<tr>
<td>Define virtualization technology.</td>
</tr>
<tr>
<td>Identify advantages and disadvantages of using virtual machines.</td>
</tr>
<tr>
<td>Identify representation of data at lowest levels.</td>
</tr>
<tr>
<td>Define <strong>programming</strong> in the context of cybersecurity.</td>
</tr>
<tr>
<td>Differentiate between computer programming languages.</td>
</tr>
<tr>
<td>Describe Python</td>
</tr>
<tr>
<td>Demonstrate Linux</td>
</tr>
<tr>
<td>Evaluate common programming flaws that lead to vulnerabilities.</td>
</tr>
<tr>
<td>Identify best practices in secure coding and design.</td>
</tr>
<tr>
<td>Identify ubiquitous computing.</td>
</tr>
<tr>
<td>Description security and privacy implications of ubiquitous computing.</td>
</tr>
<tr>
<td>Research career opportunities for cybersecurity professionals.</td>
</tr>
<tr>
<td>Examine the Career Clusters affected by current and emerging technology.</td>
</tr>
<tr>
<td>Identify the educational pathways for emerging cybersecurity professionals.</td>
</tr>
<tr>
<td>Identify career paths and job titles within the cybersecurity and/or cyber forensics industry and Career Clusters.</td>
</tr>
<tr>
<td>Research the cyber threats and security measures related to career pathways.</td>
</tr>
<tr>
<td>Identify testing skills and strategies for a certification examination.</td>
</tr>
<tr>
<td>Describe the process and requirements for obtaining industry certifications related to the Cybersecurity Fundamentals course.</td>
</tr>
</tbody>
</table>
Demonstrate the ability to complete selected practice examinations.

Successfully complete an industry certification examination representative of skills learned in this course.

**Teacher Resources**

**Instructional Scenarios**

**Risk/Vulnerabilities/Management, Oh My!**

**Duty/Concept Area(s):** Exploring Cybersecurity Fundamentals

**Scenario:**

You have been hired by the Trigon Corporation to create a series of presentations on security risks. The president wants his employees to be knowledgeable of the types of cybersecurity threats to the company and its employees.

**Big Question:**

What are risk and vulnerabilities, and how does a company manage them?

**Focused Questions:**

1. What is the definition of *risk*?
2. What is the definition of *vulnerability*?
3. Why do organizations need to manage risk?
4. Why are the basic concepts of cybersecurity risk management?

**Project-Based Assessment:**

Read the following paper: [https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204](https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204)

Create a Power Point to present to the users of Trigon. The Power Point should include an appropriate background, pictures, and the following information on the slides:

- Introduction
- Definition of *risk* and an example.
- Definition of *vulnerability* and two examples.
- Explanation of why users need to manage risk.
- Explanation of the concepts of managing risk. A slide should be done for each of these concepts and examples of where each might be used should be provided (these are the same as in economics and personal finance):
  - Risk Mitigation
  - Risk Transfer
  - Risk Avoidance
  - Risk Acceptance

**Resources:**

- Cybersecurity Risks

**Threats and Threat Actors – Not Just External Any More**

**Duty/Concept Area(s):** Describe cybersecurity threats to an organization.

**Scenario:**
You have been hired by a large bank in Virginia. They have asked you to detail what threats they might expect to their network and business. Specifically, they would like to know who might attack their network and how the attack would occur.

**Big Question:**
Can you describe the cybersecurity threats to an organization?

**Focused Questions:**
1. Who are the threat actors?
2. What are the attack types?
3. What types of malware are out there?

**Project-Based Assessment:**

Watch the following videos (Professor Messer):

  - Section 1.1 – Malware (all)
  - Section 1.2 – Attack Types (all)
  - Section 1.3 – Threat Actors

A bank with a large footprint in the Commonwealth of Virginia is potentially at risk for cyber threats.

You have been asked to write a report that details the following:

- Who are the top two threat actors?
  - Why are they the most concerning?
  - What can they affect within the network?
- What are the top five attacks the bank faces regarding its internal network?
  - How do they work?
  - Why are they the top ones?
  - How would they affect the business/network?
- What are the top two attacks to the bank’s web-facing systems?
  - How do they work?
  - What makes these attacks the most prevalent?
  - How would they affect the business/network?

For this report, follow APA format and cite a minimum of five other references.

**Resources:**

- [World’s Biggest Data Breaches & Hacks](https://www.info-is-beautiful.com/worlds-biggest-data-breaches-hacks/), Information is Beautiful
- [Cyber Org](https://www.instructure.com/cyber-org), Instructure
- [Open Web Application Security Project (OWASP) Top Ten](https://www.owasp.org/index.php/Top_Ten), OWASP Foundation

**We Have Standards?**

**Duty/Concept Area(s):** Discuss national or industry standards/regulations that relate to cybersecurity.

**Scenario:**
You would like to leave your position at the hospital to enter the field of education or pursue a position at the Department of Defense. How do you research the differences in regulations regarding cybersecurity in this field?

**Big Question:**
What are the industry standards/regulations that relate to cybersecurity?

**Focused Questions:**

1. What is PCI DSS?
2. What is FERPA?
3. What is HIPPA?
4. What is GDPR?
What is NIST?
What is ISO?

**Project-Based Assessment:**
Arrange students into groups of two or three, or make this an individual assignment. Research regulations and frameworks for security. Choose a total of ten different frameworks and provide the following information for each in chart format:

- What types of business are these targeting/required for?
- What are the overall basic requirements?
- What and who is it designed to protect?
- What are the penalties for not following the specific regulation?

**Resources:**
- [Infosecurity Magazine](https://www.infosecurity-magazine.com), Infosecurity Group
- [23 Top Cybersecurity Frameworks](https://www.cyberexperts.com), CyberExperts
- [Cybersecurity Frameworks 101 – The Complete Guide](https://www.preyproject.com), Prey Project

**Cybersecurity – Where Can They Get Me?**

**Duty/Concept Area(s):** Describe the cyberattack surface of various organizations.

**Scenario:**
You have been hired by a contractor from the Department of Defense to review their risk factors and make suggestions on how to decrease their attack surface. They have
- communications (wired/wireless)
- connections to the Internet for employees to use
- facilities within five miles of each other
- door locks as the only form of physical security into the building
- credit card payments accepted over the web.

**Big Question:**
Can you describe what cybersecurity is and what it is exactly that businesses want to protect?

**Focused Questions:**
1. What is important for companies to protect?
2. What are the differences in the definition of cybersecurity?
3. Why is cybersecurity important?

**Project-Based Assessment:**
Research how to reduce your attack surface, then review the scenario. Determine what attack areas are wide open, which ones you would fix, and how. Share these with your fellow students in a discussion.

**Resources:**
- CYBER.ORG Cyber Business Module: How Businesses Secure Information

**Cybersecurity: How to Help to Avoid a “Gotcha”?**

**Duty/Concept Area(s):** Analyze risks affecting critical infrastructure.

**Scenario:**
You have been hired by a company to make a presentation to the Department of Homeland Security about a specific piece of critical infrastructure.

**Big Question:**
What are the critical infrastructure areas found in cybersecurity? How can they be threatened, and how can they be protected?
Focused Questions:
1. What threatens our critical infrastructure?
2. What are the 16 critical infrastructure areas?
3. How are threats evolving?
4. How do those threats relate to these infrastructure areas?

Project-Based Assessment:
Arrange students into research groups of two or three to gather required information for the presentation.

Starting point: Critical Infrastructure Sectors.

- Research the selected sector.
- Create three attack scenarios that focus on ways the sector can be taken down:
  - Cyberattacks (required)
  - Terrorism
  - Pandemics
  - Weather
  - Technical failures
- Create a game plan and document the potential plans of attack.
- Create at least three methods of preventing those types of attacks.
- Present those methods as a classroom example of a presentation to the Department of Homeland Security.
Can You Secure a Home From a Cyberattack?

Duty/Concept Area(s): Understanding Cyber Threats and Vulnerabilities

Scenario:
You and your partners are developing a Blue Team defense system for a personal residence home. After reviewing the home plan, the team realizes that there are physical and digital weaknesses that need to be secured to protect the property, personal items, important documents, and digital access.

The home owners requested that the following be addressed and implemented:

- How is unauthorized access gained to the home and the home network?
- How will the home office be secured?
- Will the homeowners have access to necessary protections if they are on a budget?
- Can their home and data be protected in a way that prevents anyone from being harmed?

Big Question:
How can businesses, residences, and users protect themselves from both physical & cyber threats?
Focused Questions:
1. Why do we need to protect our system?
2. How can someone gain unauthorized access to a physical location and network?
3. Can you predict and prevent all attacks?
4. Can you make anything 100 percent secure?

Project-Based Assessment:
Complete a small group activity threat modeling a home, taking on the mindset of Blue Team to protect the home. When the activity is completed, have the groups switch plans and take on the mindset of the Red Team to determine if there are any vulnerabilities in the plans. Use the link in the resources to access the lessons.

Resources:
- The Security Mindset: Cybersecurity through Threat Modeling
- Open Source Security, pfSense, Electric Sheep Fencing, LLC

Who’s Data Is It, Anyway?
Duty/Concept Area(s): Exploring Ethics as it Relates to Cybersecurity

Scenario:
One responsibility of the department store’s security team is to monitor free Wi-Fi traffic to make sure no one is conducting illegal activity over the store’s wireless network. In the course of normal monitoring activities, the security team intercepts emails between two people who are experiencing serious financial problems. The contents of these emails are in plain text and can be easily viewed by common packet sniffing tools.

Both people have recently been laid off from their jobs. The emails include details such as the couple’s car recently being repossessed and a pending foreclosure on their house. While it seems unlikely that the couple will be able to pay off any future credit card bills, the couple’s store credit account is still current and in good standing. The couple gathers a rather large and expensive selection of products, and they tell the store clerk to charge the items to their store credit account. The store’s management, however, has already closed out the couple’s account based on the intercepted emails.

Big Question:
Can the store ethically intercept private conversations taking place across a network connection that they own and provide to customers free of charge?

Focused Questions:
1. What expectation of privacy does the couple have in this situation?
2. What could the couple do to protect themselves from such unwanted scrutiny?
3. How does the store balance its obligation to prevent illegal activity across its network with a customer’s right to privacy?

Project-Based Assessment:
Class discussion/role play illustrating obligations and rights of both the customer and the store.

What’s the Big Deal About Data Privacy?
Duty/Concept Area(s): Exploring Data Privacy

Scenario:
You have been hired to review a client's online privacy. They have been hacked, and you are looking at their potential profile and posting issues to help them have a more secure online experience. The client is also asking how their information can be exploited and used by other people and companies.

Big Question:
How can users protect themselves and their data from being exploited?
Focused Questions:
1. What are the risks associated with posting personal information?
2. How do you protect your privacy on social media and commercial websites?
3. What kind of information is being collected on the sites, platforms, and browsers that you use?
4. What are the benefits and risks of online tracking for users?
5. How do you protect yourself from online tracking?

Project-Based Assessment:
- In a small group, review a fictional public social media network profile. Prepare a presentation
  - reporting potential privacy issues
  - offering suggestions on how to protect from online tracking from other people and companies
  - offering solutions to ensure private information is secure.
- Use the first link under Resources to access the lesson and examples of profiles for this assessment. You may also create multiple profiles for each group to research and present.

Links have been provided below to use as projects, activities, and assessments.

Resources:
- The Invisible Machine: Big Data and You, The eQuality Project, Media Smarts
- 23 Great Lesson Plans for Internet Safety, Common Sense Media
- The Big Data Dilemma, Common Sense Media
- Debating the Privacy Line, Common Sense Media
- Privacy and Internet Life: Lesson Plan for Intermediate Classrooms, Common Sense Media
- Privacy Badger, Electronic Frontier Foundation

Big Data, Little Data

Duty/Concept Area(s): Examining Data Security as it Relates to Cybersecurity

Scenario:
You decide you want to purchase a Bluetooth speaker. You visit Amazon.com first. When you enter “Bluetooth Speaker” into the search bar, you receive a lot of results. You also find you can filter your criteria by
- price
- speed of shipment
- type of phones compatibility
- special features
- manufacturer
- a number of other criteria.

When you create a Google search for “Bluetooth Speaker” the results are very different, and you can’t really filter them in the same ways. Why is this?

Big Question:
In what ways are companies able to tailor data to your specifications and interests?

Focused Questions:
1. Where is this data being stored? Is it a type of software?
2. How can the specified criteria be filtered so quickly?
3. Why do different kinds of searches vary so much?
4. Are there different ways of accessing all of this data?

Project-Based Assessment:
Create a simple relational database and design a query that will filter the data based on user selections. It should
- Demonstrate ways in which the data could be “tainted” to cause it to not function properly.
• Examine ways to make queries less exact (i.e. like or wildcard queries)
• Look at the difference between a natural language query and a SQL query.

Resources:
• https://computer.howstuffworks.com/question599.htm
• https://www.dummies.com/software/microsoft-office/access-2019-how-to-create-an-access-database/

Do I Really Need to Give Access to That?

Duty/Concept Area(s): 84 – 93/Securing Operating Systems

Scenario:
John plugs his smartphone into his school laptop. A message box appears asking, “Do you want to download your photos onto this device?” What should he do?

Big Question:
Why is it important to know about security parameters like the different types of access controls (e.g. rights and permissions)?

Focused Questions:
• Different operating systems allow users to automatically upload files from one device to another. Why should this be important to you?
• Looking at this scenario, what would happen if John clicks “Allow”?
• Would John still have privacy rights to his photos if they are uploaded onto his school computer?
• Can anyone who has access to his laptop now see those photos?
• What can you do to keep your information private?

Resources:
Show App permissions - What you need to know and discuss why companies harvest your data.

Internet of Things - How does Alexa really work?

Duty/Concept Area(s): Exploring Cybersecurity Implications for Current and Emerging Technologies

Scenario:
Susie has an Amazon Alexa device in her home, and she uses it to play her favorite music and call her friends. Amazon Alexa is an example of an Internet of Things (IoT). What are the pros and cons of this type of IoT?

Big Question:
What are the pros and cons of the Amazon Alexa IoT?

Focused Questions:
1. Is an IoT like Amazon Alexa always listening to you? If so, is that data stored? How is it used?
2. Can Amazon Alexa be hacked? How? Why would someone want to hack your Amazon Alexa?
3. How do you know if someone is dropping in on Amazon Alexa?

Project-Based Assessment:
• Have your students research the focus questions and share the information with the rest of the class. This can be a project or a quick 15-minute exercise.
Cyber Security and Cyber Forensics Infusion Units

Cyber Security and Cyber Forensic Infusion Units (CYBR) were designed to be infused with designated CTE courses to help students in those programs achieve additional, focused, validated tasks/competencies in personal and professional cyber security skills. These units are not mandatory, and, as such, the tasks/competencies are marked as "optional," to be taught at the instructor's discretion.

Customer Service Infusion Units

Customer Service Infusion Units (CSIU) were designed to be infused with designated CTE courses to help students in those programs achieve additional, focused, validated tasks/competencies in customer service. These units are not mandatory, and, as such, the tasks/competencies are marked as "optional," to be taught at the instructor's discretion.

Entrepreneurship Infusion Units

Entrepreneurship Infusion Units may be used to help students achieve additional, focused competencies and enhance the validated tasks/competencies related to identifying and starting a new business venture. Because the unit is a complement to certain designated courses and is not mandatory, all tasks/competencies are marked “optional.”
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 Operations (6304/36 weeks)
- Cybersecurity 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

<table>
<thead>
<tr>
<th>Pathway</th>
<th>Occupations</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Security</td>
<td>Military Intelligence Specialist</td>
</tr>
<tr>
<td>Planning</td>
<td>Interviewer</td>
</tr>
<tr>
<td>Public Management and</td>
<td>Government Accountant/Auditor</td>
</tr>
<tr>
<td>Administration</td>
<td></td>
</tr>
<tr>
<td>Regulation</td>
<td>Cyber Crime Investigator Financial Analyst Privacy Compliance Manager</td>
</tr>
</tbody>
</table>

Career Cluster: Government and Public Administration

<table>
<thead>
<tr>
<th>Pathway</th>
<th>Occupations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue and Taxation</td>
<td>Financial Analyst</td>
</tr>
<tr>
<td>Pathway</td>
<td>Occupations</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 |