Department of Education | College, Career and Technical Education

Published for 2020-21 school year.

Cybersecurity I

Primary Career Cluster:	Information Technology
Course Contact:	CTE.Standards@tn.gov
Course Code(s):	C10H19
Prerequisite(s):	*Algebra I* (G02X02, G02H00), *Computer Science Foundations* (C10H11)
Credit:	1
Grade Level:	10
Focus Elective Graduation Requirements:	This course satisfies one of three credits required for an elective focus when taken in conjunction with other *Information Technology* courses.
Program of study (POS) Concentrator:	This course satisfies one out of two required courses that meet the Perkins V concentrator definition, when taken in sequence in the approved program of study.
Programs of Study and Sequence:	This is the second course in the *Cybersecurity* program of study.
Aligned Student Organization(s)	SkillsUSA: http://www.tnskillsusa.com Technology Student Association (TSA): http://www.tntsa.org
Coordinating Work-Based Learning:	Teachers are encouraged to use embedded WBL activities such as informational interviewing, job shadowing, and career mentoring. For information, visit https://www.tn.gov/content/tn/education/career-and-technical-education/work-based-learning.html
Available Student Industry Certifications:	Students are encouraged to demonstrate mastery of knowledge and skills learned in this course by earning the appropriate, aligned department-promoted industry certifications. Access the promoted list here for more information.
Teacher Endorsement(s):	037, 041, 055, 056, 057, 152, 153, 203, 204, 311, 413, 434, 435, 436, 470, 474, 475, 476, 477, 582, 595, 740, 742, 952, 953
Required Teacher Certifications/Training:	All endorsements except for 742 will require either the NOCTI test code 5906: Computer Programming certification **or** the equivalent of twelve semester hours of computer course work including at least six hours of programming language.
Teacher Resources:	https://www.tn.gov/education/career-and-technical-education/career-clusters/cte-cluster-information-technology.html

Course Description

Cybersecurity I is a course intended to teach students the basic concepts of cybersecurity. The course places an emphasis on security integration, application of cybersecurity practices and devices, ethics, and best practices management. The fundamental skills in this course cover both in house and external threats to network security and design, how to enforce network level security policies, and how to safeguard an organization's information. Upon completion of this course, proficient students will be demonstrate and understanding of cybersecurity concepts, identify fundamental principles of networking systems, understand network infrastructure and network security, and be able to demonstrate how to implement various aspects of security within a networking system.

Program of Study Application

This program offers a sequence of courses that provides coherent and rigorous content aligned with challenging academic standards and relevant technical knowledge and skills needed to prepare for further education and cybersecurity-related careers in the Information Technology career cluster. This is the second course in the *Cybersecurity* program of study. For more information on the benefits and requirements of implementing this program in full, please visit the Information Technology website at https://www.tn.gov/education/career-and-technical-education/career-clusters/cte-cluster-information-technology.html.

Course Standards

Cybersecurity Fundamental Concepts

1) Using websites and journals from professional organizations related to information technology, analyze ethical security practices, including but not limited to the issues of data security, confidentiality, integrity, availability, authentication, nonrepudiation, physical security, HIPPA Laws, Payment Card Industry (PCI) Compliance, and the importance of ISO27000 standards.

2) Using news articles, research current events on breaches; focus on particular Information Assurance (IA) areas that were compromised. For example, research and report on the effects of unethical security breaches on a business citing specific textual evidence.

3) Consult a variety of sources to analyze security threats, vulnerabilities, and exploits. Research common ways that threats, vulnerabilities, and exploits impact an organization. For example, research and report on the threats, vulnerabilities, and exploit(s) used in a recent high profile breach.

Risk Management Techniques

4) Read and interpret technical information to define risk management and how it applies to information security. Examine a case study of a company using a systematic approach for the identification, assessment and management of information security risks and compile a brief narrative summarizing conclusions.

5) Preform a simulated risk assessment by using the common industry framework from ISO. Analyze and describe the risk mitigation techniques of acceptance, mitigation, avoidance, and transfer.

Access Controls

6) Gather relevant information from textbooks and online resources to explain the core concepts of access control as they relate to authentication and authorization. Create an infographic a security analyst could use as a guide.

7) Interpret instructional materials to analyze and describe the core principles of access controls. Instructional material may include textbooks, manuals, websites, video tutorials, and more. For example, analyze the use of administrative, logical (technical) and physical controls applied to systems, and organizations.

8) Demonstrate the use of access controls that apply to user account management, including basic and advanced techniques. Drawing on evidence from textbooks and other resources, evaluate the effectiveness of the controls and incorporate feedback when refining techniques.

Fundamental Principles of Networking

9) Prepare informational artifacts (e.g., brochure, poster, fact sheet, narrative, or presentation) for the following LAN topics:
    a. Identify and describe common LAN methodologies
    b. Analyze the various LAN topologies including perimeter networks which may include the use of a DMZ.
    c. Indicate and explain the standards of Ethernet.
    d. Describe the characteristics of LAN cabling.

10) Explain the industry standards used in wireless networks including security protocols used to protect the wireless network. Read and interpret trade journals, assessing the usefulness of each source, to describe the impact the protocol has had on a particular network. For example, cite evidence from trade journals to explain the Secure Socket Layer (SSL) and Transport Layer Security (TLS) Protocols and their impact on the security of wireless networks.

11) Consult a variety of sources to describe how routing protocols are used and the differences between static and dynamic methods of routing. Sources may include textbooks, manuals, websites, video tutorials, and more. Create a visual display with accompanying text comparing and contrasting these two methods.

12) Create an illustrative guide that explains how to install and configure Routing and Remote Access Service (RRAS) to function as a network router and how to install and configure Routing Information Protocols.

13) Choose between technologies and topologies utilized for WAN networks and justify the choices Make a written case for selecting one technology and topologies over another, highlighting the features of each and citing resources to validate claims.

14) Explain how the different types of personal and small business internet connectivity has changed throughout history, and identify current internet systems most commonly used. Consult internet forums, textbooks, industry journals and other instructional materials, assessing the usefulness of each source, to describe the impact these changes have made. Create and present a document and/or illustration depicting the timeline of development that led to modern-day internet systems citing specific textual evidence.

Fundamental Principles of Open Systems and Internet Protocol

15) Identify, describe, and effectively summarize the common OSI model and the functions used by each layer. Create a written report or visual depiction outlining the characteristics and properties of each.

16) Research and create an informational artifact (e.g., brochure, poster, fact sheet, narrative, or presentation) analyzing and describing the differences between the TCP/IP and OSI models for networking.

17) Define and describe the various services used by networks for the transmission of data such as DNS, NAT, and DHCP. Create a graphic illustration showing the roles of each service and describe their differences.

18) Analyze the differences among the addressing techniques used by networks, including IPv4 and basic IPv6. Write a brief paper that discusses the differences. Provide specific examples to support the claims.

19) Using instructional materials, analyze then demonstrate the use of subnets in an organizations network environment. For example, create a simple network using subnets for different organizational locations. Instructional materials may include textbooks, instructional manuals, websites, video tutorials, and more.

20) Research the features and requirements of a working model of a client server network and how services function in a networked windows environment. Drawing on multiple resources, demonstrate installation of the various network services in the client server network.

Network Infrastructures and Network Security

21) Compare and contrast the differences and uses of the Internet, Intranets, and Extranets. Citing specific examples, create an illustrative guide that outlines the benefits of each and major similarities and differences.

22) Research and describe the most common various methods and technology used to secure networks. Investigate and distinguish among the following common methods to secure a network.
    a. VPNs for remote access
    b. Firewalls
    c. Perimeter network designs
    d. Preventative technologies

Fundamental Network Components of Cybersecurity

23) Research the different applications of network security devices. Create a table or other graphic organizer that lists examples of each device and details their purpose, characteristics, and proper maintenance. Demonstrate proper installation and configuration of each device while using the appropriate media.
    a. Optical drives
    b. Combo drives and burners
    c. Connection types
    d. Hard drives
    e. Solid state / flash drives
    f. RAID types
    g. Floppy drive
    h. Tape drive
    i. Media capacity

24) Demonstrate secure networking techniques by designing a simple secure network. For example, show how the various security protocols, technology, and designs protect an organizations network.

Basic and Advanced Command Prompts

25) Synthesize information from a range of sources to analyze the various networking commands used to test and examine networks. Using domain-specific terminology, explain to a technical audience the distinguishing features of each command that make one more appropriate for certain types of applications.

26) Analyze and research the features and uses of command line utilities to configure and examine networking services and construct a flow chart that a security analyst could reference.

Application Security and Host Systems

27) Explore and identify various operating and file systems used in networks. Create a chart to define the pros and cons of how these systems are designed to provide the security necessary in a multiuser environment, citing examples of when each is used.

28) Research and describe the most common security threats to computer systems, such as social engineering, malware, phishing, viruses, etc. Investigate and distinguish among the following common prevention methods to secure a computer system. For a given scenario, identify the most applicable best practice to secure a workstation as well as describe methods for data destruction and disposal. Implement these practices and write a justification for each scenario solution. Provide supporting evidence for each solution, drawing on technical texts and industry standards. Prevention methods include:
    a. Physical security (e.g., lock doors, tailgating, biometrics, badges, key fobs, retinal, etc.)
    b. Digital security (e.g., antivirus, firewalls, antispyware, user authentication, etc.)
    c. User education

d. Principles of least privilege

29) Using news articles and instructional materials, research and report on recent threats and vulnerabilities to systems in networking environments making reference to the top application vulnerabilities and how they are used to exploit systems and networking resources.

30) Differentiate between threats and vulnerabilities and what constitutes a network attack and identify how to differentiate between the different types of application attacks. Citing specific examples, create an illustrative guide that outlines major similarities and differences.

31) Identify and explain ways to install and configure anti-virus software. Demonstrate the installation of security software design to protect systems on the network. Upon completion of the work, write an explanation and justify the actions by citing supporting evidence from technical manuals and industry standards.

Security Administration

32) Research the features and requirements of common security procedures used to protect system resources on a network. Drawing on multiple resources, explain why it is important to know this information when developing a security procedure.

33) Identify and describe the differences among various methods to create baseline security measures. Utilizing existing tools on a system, such as the Microsoft Baseline Security Analyzer, outline the steps taken to create a security measure.

34) Research the following storage devices and backup media. Create a table or other graphic organizer that lists examples of each device and details their purpose, characteristics, proper maintenance, and methods used to back up and protect data from unauthorized use and access of data.
    a. Optical drives
    b. Combo drives and burners
    c. Connection types
    d. Hard drives
    e. Solid state / flash drives
    f. RAID types
    g. Floppy drive
    h. Tape drive
    i. Media capacity

35) Demonstrate the methods used to protect against unauthorized use of files. Configure file and folder permissions using both Windows and Linux environments.

36) Analyze various protocols and services used by systems for securing them in a network environment. Create a table that lists the purpose and distinguishing features of each protocol and service.

Cryptology

37) Drawing on multiple sources (i.e., internet, textbooks, videos, and journals), research the history of cryptology. Create a timeline or infographic, illustrating cryptology's historical evolution from its inception to the present time including but not limited to public key infrastructures, asymmetric and symmetric encryptions. Provide examples drawn from the research to support claims.

38) Analyze common methods and use of cryptology to protect data. Compare and contrast general methods used, and explain how their designs and functionalities support the security of data.

Standards Alignment Notes

*References to other standards include:

- P21: Partnership for 21st Century Skills Framework for 21st Century Learning
    - Note: While not all standards are specifically aligned, teachers will find the framework helpful for setting expectations for student behavior in their classroom and practicing specific career readiness skills.