Foundations of Cybersecurity

Subject: Career and Technical Education
Grade: 09
Expectations: 107
Breakouts: 274

(a) Introduction.

1. Career and technical education instruction provides content aligned with challenging academic standards, industry and relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and emerging professions.

2. The Science, Technology, Engineering, and Mathematics (STEM) Career Cluster focuses on planning, managing, and providing scientific research and professional and technical services such as laboratory and testing services and research and development services.

3. Cybersecurity is a critical discipline concerned with safeguarding computers, networks, programs, and data from unauthorized access. As a field, it has gained prominence with the expansion of a globally connected society. As computing has become more sophisticated, so too have the abilities of adversaries looking to penetrate networks and access systems and sensitive information. Cybersecurity professionals prevent, detect, and respond to minimize disruptions to governments, organizations, and individuals.

4. In the Foundations of Cybersecurity course, students will develop the knowledge and skills needed to explore fundamental concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will review and explore security policies designed to mitigate risks. The skills obtained in this course prepare students for additional study in cybersecurity. A variety of courses are available to students interested in this field. Foundations of Cybersecurity may serve as an introductory course in this field of study.

5. Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.

6. Statements that contain the word "including" reference content that must be mastered, while those containing the phrase "such as" are intended as possible illustrative examples.

(b) Knowledge and Skills Statements

(1) Employability skills. The student demonstrates necessary skills for career development and successful completion of course outcomes. The student is expected to:

(A) identify and demonstrate employable work behaviors such as regular attendance, punctuality, maintenance of a professional work environment, and effective written and verbal communication;

(i) identify employable work behaviors

(ii) demonstrate employable work behaviors

(B) identify and demonstrate positive personal qualities such as authenticity, resilience, initiative, and a willingness to learn new knowledge and skills;

(i) identify positive personal qualities

(ii) demonstrate positive personal qualities

(C) solve problems and think critically;

(i) solve problems

(ii) think critically

(D) demonstrate leadership skills and function effectively as a team member; and

(i) demonstrate leadership skills

(ii) function effectively as a team member

(E) demonstrate an understanding of ethical and legal responsibilities and ramifications in relation to the field of cybersecurity.

(i) demonstrate an understanding of ethical responsibilities in relation to the field of cybersecurity

(ii) demonstrate an understanding of ethical ramifications in relation to the field of cybersecurity.

(iii) demonstrate an understanding of legal responsibilities in relation to the field of cybersecurity

(iv) demonstrate an understanding of legal ramifications in relation to the field of cybersecurity

(2) Professional awareness. The student identifies various employment opportunities and requirements in the cybersecurity field. The student is expected to:

(A) identify job and internship opportunities and accompanying job duties and tasks;

(i) identify job opportunities

(ii) identify internship opportunities

(iii) identify accompanying job duties

(iv) identify accompanying tasks

(B) research careers in cybersecurity and information security and develop professional profiles that match education and job skills required for obtaining a job in both the public and private sectors;

(i) research careers in cybersecurity

(ii) research careers in information security

(iii) develop professional profiles that match education required for obtaining a job in the public sector

(iv) develop professional profiles that match education required for obtaining a job in the private sector

(v) develop professional profiles that match job skills required for obtaining a job in the public sector

(vi) develop professional profiles that match job skills required for obtaining a job in the private sector

(C) identify and discuss certifications for cybersecurity-related careers; and

(i) identify certifications for cybersecurity-related careers

(ii) discuss certifications for cybersecurity-related careers

(D) explain the different types of services and roles found within a cybersecurity functional area such as a security operations center (SOC).

(i) explain the different types of services found within a cybersecurity functional area

(ii) explain the different types of roles found within a cybersecurity functional area

(3) Ethics and laws. The student understands ethical and current legal standards, rights and restrictions governing technology, technology systems, digital media, and the use of social media. The student is expected to:

(A) demonstrate and advocate for ethical and legal behaviors both online and offline among peers, family, community, and employers;

(i) demonstrate ethical behavior online among peers

(ii) demonstrate ethical behavior online among family

(iii) demonstrate ethical behavior online among community

(iv) demonstrate ethical behavior online among employers

(v) demonstrate ethical behavior offline among peers

(vi) demonstrate ethical behavior offline among family

(vii) demonstrate ethical behavior offline among community

(viii) demonstrate ethical behavior offline among employers

(ix) demonstrate legal behavior online among peers

(x) demonstrate legal behavior online among family

(xi) demonstrate legal behavior online among community

(xii) demonstrate legal behavior online among employers

(xiii) demonstrate legal behavior offline among peers

(xiv) demonstrate legal behavior offline among family

(xv) demonstrate legal behavior offline among community

(xvi) demonstrate legal behavior offline among employers

(xvii) advocate for ethical behavior online among peers

(xviii) advocate for ethical behavior online among family

(xix) advocate for ethical behavior online among community

(xx) advocate for ethical behavior online among employers

(xxi) advocate for ethical behavior offline among peers

(xxii) advocate for ethical behavior offline among family

(xxiii) advocate for ethical behavior offline among community

(xxiv) advocate for ethical behavior offline among employers

(xxv) advocate for legal behavior online among peers

(xxvi) advocate for legal behavior online among family

(xxvii) advocate for legal behavior online among community

(xxviii) advocate for legal behavior online among employers

(xxix) advocate for legal behavior offline among peers

(xxx) advocate for legal behavior offline among family

(xxxi) advocate for legal behavior offline among community

(xxxii) advocate for legal behavior offline among employers

(B) investigate and analyze local, state, national, and international cybersecurity laws such as the USA PATRIOT Act of 2001, General Data Protection Regulation, Digital Millennium Copyright Act, Computer Fraud and Abuse Act, and Health Insurance Portability and Accountability Act of 1996 (HIPAA);

(i) investigate local laws

(ii) investigate state laws

(iii) investigate national laws

(iv) investigate international laws

(v) analyze local laws

(vi) analyze state laws

(vii) analyze national laws

(viii) analyze international laws

(C) investigate and analyze noteworthy incidents or events regarding cybersecurity;

(i) investigate noteworthy incidents or events regarding cybersecurity

(ii) analyze noteworthy incidents or events regarding cybersecurity

(D) communicate an understanding of ethical and legal behavior when presented with various scenarios related to cybersecurity activities;

(i) communicate an understanding of ethical behavior when presented with various scenarios related to cybersecurity activities

(ii) communicate an understanding of legal behavior when presented with various scenarios related to cybersecurity activities

(E) define and identify tactics used in an incident such as social engineering, malware, denial of service, spoofing, and data vandalism; and

(i) define tactics used in an incident

(ii) identify tactics used in an incident

(F) identify and use appropriate methods for citing sources.

(i) identify appropriate methods for citing sources

(ii) use appropriate methods for citing sources

(4) Ethics and laws. The student differentiates between ethical and malicious hacking. The student is expected to:

(A) identify motivations and perspectives for hacking;

(i) identify motivations for hacking

(ii) identify perspectives for hacking

(B) distinguish between types of threat actors such as hacktivists, criminals, state-sponsored actors, and foreign governments;

(i) distinguish between types of threat actors

(C) identify and describe the impact of cyberattacks on the global community, society, and individuals;

(i) identify the impact of cyberattacks on the global community

(ii) identify the impact of cyberattacks on society

(iii) identify the impact of cyberattacks on individuals

(iv) describe the impact of cyberattacks on the global community

(v) describe the impact of cyberattacks on society

(vi) describe the impact of cyberattacks on individuals

(D) differentiate between industry terminology for types of hackers such as black hats, white hats, and gray hats; and

(i) differentiate between industry terminology for types of hackers

(E) determine and describe possible outcomes and legal ramifications of ethical versus malicious hacking practices.

(i) determine possible outcomes of ethical versus malicious hacking practices

(ii) determine legal ramifications of ethical versus malicious hacking practices

(iii) describe possible outcomes of ethical versus malicious hacking practices

(iv) describe legal ramifications of ethical versus malicious hacking practices

(5) Ethics and laws. The student identifies and defines cyberterrorism and counterterrorism. The student is expected to:

(A) define cyberterrorism;

(i) define state-sponsored cyberterrorism

(ii) define hacktivism

(B) compare and contrast physical terrorism and cyberterrorism, including domestic and foreign actors;

(i) compare and contrast physical terrorism and cyberterrorism, including domestic actors

(ii) compare and contrast physical terrorism and cyberterrorism, including foreign actors

(C) define and explain intelligence gathering;

(i) define intelligence gathering

(ii) explain intelligence gathering

(D) explain the role of cyber defense in protecting national interests and corporations;

(i) explain the role of cyber defense in protecting national interests

(ii) explain the role of cyber defense in protecting corporations

(E) explain the role of cyber defense in society and the global economy; and

(i) explain the role of cyber defense in society

(ii) explain the role of cyber defense in the global economy

(F) explain the importance of protecting public infrastructures such as electrical power grids, water systems, pipelines, transportation, and power generation facilities from cyberterrorism.

(i) explain the importance of protecting public infrastructures

(6) Digital citizenship. The student understands and demonstrates the social responsibility of end users regarding significant issues related to digital technology, digital hygiene, and cyberbullying. The student is expected to:

(A) identify and understand the nature and value of privacy;

(i) identify the nature of privacy

(ii) identify the value of privacy

(iii) understand the nature of privacy

(iv) understand the value of privacy

(B) analyze the positive and negative implications of a digital footprint and the maintenance and monitoring of an online presence;

(i) analyze the positive implications of a digital footprint

(ii) analyze the negative implications of a digital footprint

(iii) analyze the maintenance of an online presence

(iv) analyze the monitoring of an online presence

(C) discuss the role and impact of technology on privacy;

(i) discuss the role of technology on privacy

(ii) discuss the impact of technology on privacy

(D) identify the signs, emotional effects, and legal consequences of cyberbullying and cyberstalking; and

(i) identify the signs of cyberbullying

(ii) identify the emotional effects of cyberbullying

(iii) identify the legal consequences of cyberbullying

(iv) identify the signs of cyberstalking

(v) identify the emotional effects of cyberstalking

(vi) identify the legal consequences of cyberstalking

(E) identify and discuss effective ways to deter and report cyberbullying.

(i) identify effective ways to deter cyberbullying

(ii) identify effective ways to report cyberbullying

(iii) discuss effective ways to deter cyberbullying

(iv) discuss effective ways to report cyberbullying

(7) Digital citizenship. The student understands the implications of sharing information and access with others. The student is expected to:

(A) define personally identifiable information (PII);

(i) define personally identifiable information (PII)

(B) evaluate the risks and benefits of sharing PII;

(i) evaluate the risks and benefits of sharing PII

(C) describe the impact of granting applications unnecessary permissions such as mobile devices accessing camera and contacts;

(i) describe the impact of granting applications unnecessary permissions

(D) describe the risks of granting third parties access to personal and proprietary data on social media and systems; and

(i) describe the risks of granting third parties access to personal data on social media and systems

(ii) describe the risks of granting third parties access to proprietary data on social media and systems

(E) describe the risks involved with accepting Terms of Service (ToS) or End User License Agreements (EULA) without a basic understanding of the terms or agreements.

(i) describe the risks involved with accepting Terms of Service (ToS) or End User License Agreements (EULA) without a basic understanding of the terms or agreements

(8) Cybersecurity skills. The student understands basic cybersecurity concepts and definitions. The student is expected to:

(A) define cybersecurity and information security;

(i) define cybersecurity security

(ii) define information security

(B) identify basic risk management and risk assessment principles related to cybersecurity threats and vulnerabilities, including the Zero Trust model;

(i) identify basic risk management principles related to cybersecurity threats and vulnerabilities, including the Zero Trust model

(ii) identify basic risk assessment principles related to cybersecurity threats and vulnerabilities, including the Zero Trust model

(C) explain the fundamental concepts of confidentiality, integrity, and availability (CIA triad);

(i) explain the fundamental concepts of confidentiality

(ii) explain the fundamental concepts of integrity

(iii) explain the fundamental concepts of availability

(D) describe the trade-offs between convenience and security;

(i) describe the trade-offs between convenience and security

(E) identify and analyze cybersecurity breaches and incident responses;

(i) identify cybersecurity breaches and incident responses

(ii) identify incident responses

(iii) analyze cybersecurity breaches and incident responses

(iv) analyze incident responses

(F) identify and analyze security challenges in domains such as physical, network, cloud, and web;

(i) identify security challenges in domains

(ii) analyze security challenges in domains

(G) define and discuss challenges faced by cybersecurity professionals such as internal and external threats;

(i) define challenges faced by cybersecurity professionals;

(ii) discuss challenges faced by cybersecurity professionals

(H) identify indicators of compromise such as common risks, warning signs, and alerts of compromised systems;

(i) identify indicators of compromise

(I) explore and discuss the vulnerabilities of network-connected devices such as Internet of Things (IoT);

(i) explore the vulnerabilities of network-connected devices

(ii) discuss the vulnerabilities of network-connected devices

(J) use appropriate cybersecurity terminology;

(i) use appropriate cybersecurity terminology

(K) explain the concept of penetration testing, including tools and techniques; and

(i) explain the concept of penetration testing, including tools

(ii) explain the concept of penetration testing, including techniques

(L) explore and identify common industry frameworks such as MITRE ATT&CKTM , MITRE Engage TM , and Cyber Kill Chain, and the Diamond Model.

(i) explore common industry frameworks

(ii) identify common industry frameworks

(9) Cybersecurity skills. The student understands and explains various types of malicious software (malware). The student is expected to:

(A) define malware, including spyware, ransomware, viruses, and rootkits;

(i) define malware, including spyware

(ii) define malware, including ransomware

(iii) define malware, including viruses

(iv) define malware, including rootkits

(B) identify the transmission and function of malware such as trojan horses, worms, and viruses;

(i) identify the transmission of malware

(ii) identify the function of malware

(C) discuss the impact of malware and the model of "as a service";

(i) discuss the impact of malware

(ii) discuss the model of [malware] "as a service"

(D) explain the role of reverse engineering for the detection of malware and viruses; and

(i) explain the role of reverse engineering for the detection of malware

(ii) explain the role of reverse engineering for the detection of viruses

(E) describe free and commercial antivirus and anti-malware software also known as Endpoint Detection and Response software.

(i) describe free antivirus and anti-malware software also known as Endpoint Detection and Response software

(ii) describe commercial antivirus and anti-malware software also known as Endpoint Detection and Response software

(10) Cybersecurity skills. The student understands and demonstrates knowledge of techniques and strategies to prevent a system from being compromised. The student is expected to:

(A) define system hardening;

(i) define system hardening

(B) use basic system administration privileges;

(i) use basic system administration privileges

(C) explain the importance of patching operating systems;

(i) explain the importance of patching operating systems

(D) explain the importance of software updates;

(i) explain the importance of software updates

(E) describe standard practices to configure system services;

(i) describe standard practices to configure system services

(F) explain the importance of backup files;

(i) explain the importance of backup files

(G) research and explain standard practices for securing computers, networks, and operating systems, including the concept of least privilege; and

(i) research standard practices for securing computers

(ii) explain standard practices for securing networks

(iii) explain standard practices for securing operating systems, including the concept of least privilege

(H) identify vulnerabilities caused by a lack of cybersecurity awareness and training such as weaknesses posed by individuals within an organization.

(i) identify vulnerabilities caused by a lack of cybersecurity awareness

(ii) identify vulnerabilities caused by a lack of cybersecurity training

(11) Cybersecurity skills. The student understands basic network operations. The student is expected to:

(A) identify basic network devices, including routers and switches;

(i) identify basic network devices, including routers

(ii) identify basic network devices, including switches

(B) define network addressing;

(i) define network addressing

(C) analyze incoming and outgoing rules for traffic passing through a firewall;

(i) analyze incoming rules for traffic passing through a firewall

(ii) analyze outgoing rules for traffic passing through a firewall

(D) identify well known ports by number and service provided, including port 22 (Secure Shell Protocol/ssh), port 80 (Hypertext Transfer Protocol/http), and port 443 (Hypertext Transfer Protocol Secure/https);

(i) identify well known ports by number and service provided, including port 22 (Secure Shell Protocol/ssh)

(ii) identify well known ports by number and service provided, including port 80 (Hypertext Transfer Protocol/http)

(iii) identify well known ports by number and service provided, including port 443 (Hypertext Transfer Protocol Secure/https)

(E) identify commonly exploited ports and services, including ports 20 and 21 (File Transfer Protocol/ftp), port 23 (telnet protocol), and port 3389 (Remote Desktop Protocol/rdp); and

(i) identify commonly exploited ports and services, including ports 20 and 21 (File Transfer Protocol/ftp)

(ii) identify commonly exploited ports and services, including port 23 (telnet protocol)

(iii) identify commonly exploited ports and services, including port 3389 (Remote Desktop Protocol/rdp)

(F) identify common tools for monitoring ports and network traffic.

(i) identify common tools for monitoring ports

(ii) identify common tools for monitoring network traffic.

(12) Cybersecurity skills. The student identifies standard practices of system administration. The student is expected to:

(A) define what constitutes a secure password;

(i) define what constitutes a secure password

(B) create a secure password policy, including length, complexity, account lockout, and rotation;

(i) create a secure password policy, including length

(ii) create a secure password policy, including complexity

(iii) create a secure password policy, including account lockout

(iv) create a secure password policy, including rotation

(C) identify methods of password cracking such as brute force and dictionary attacks; and

(i) identify methods of password cracking

(D) examine and configure security options to allow and restrict access based on user roles.

(i) examine security options to allow access based on user roles

(ii) examine security options to restrict access based on user roles

(iii) configure security options to allow access based on user roles

(iv) configure security options to restrict access based on user roles

(13) Cybersecurity skills. The student demonstrates necessary steps to maintain user access on the system. The student is expected to:

(A) identify different types of user accounts and groups on an operating system;

(i) identify different types of user accounts on an operating system

(ii) identify different types of user groups on an operating system

(B) explain the fundamental concepts and standard practices related to access control, including authentication, authorization, and auditing;

(i) explain the fundamental concepts related to access control, including authentication

(ii) explain the fundamental concepts related to authorization

(iii) explain the fundamental concepts related to auditing

(iv) explain the standard practices related to access control, including authentication

(v) explain the standard practices related to authorization

(vi) explain the standard practices related to auditing

(C) compare methods for single- and multi-factor authentication such as passwords, biometrics, personal identification numbers (PINs), secure tokens, and other passwordless authentication methods;

(i) compare methods for single- and multi-factor authentication

(D) define and explain the purpose and benefits of an air-gapped computer; and

(i) define the purpose of an air-gapped computer

(ii) define the benefits of an air-gapped computer

(iii) explain the purpose of an air-gapped computer

(iv) explain the benefits of an air-gapped computer

(E) explain how hashes and checksums may be used to validate the integrity of transferred data.

(i) explain how hashes may be used to validate the integrity of transferred data

(ii) explain how checksums may be used to validate the integrity of transferred data

(14) Cybersecurity skills. The student explores the field of digital forensics. The student is expected to:

(A) explain the importance of digital forensics to organizations, private citizens, and the public sector;

(i) explain the importance of digital forensics to organizations

(ii) explain the importance of digital forensics to private citizens

(iii) explain the importance of digital forensics to the public sector

(B) identify the role of chain of custody in digital forensics;

(i) identify the role of chain of custody in digital forensics

(C) explain the four steps of the forensics process, including collection, examination, analysis, and reporting;

(i) explain the four steps of the forensics process, including collection

(ii) explain the four steps of the forensics process, including examination

(iii) explain the four steps of the forensics process, including analysis

(iv) explain the four steps of the forensics process, including reporting

(D) identify when a digital forensics investigation is necessary;

(i) identify when a digital forensics investigation is necessary

(E) identify information that can be recovered from digital forensics investigations such as metadata and event logs; and

(i) identify information that can be recovered from digital forensics investigations

(F) analyze the purpose of event logs and identify suspicious activity.

(i) analyze the purpose of event logs

(ii) identify suspicious activity

(15) Cybersecurity skills. The student explores the operations of cryptography. The student is expected to:

(A) explain the purpose of cryptography and encrypting data;

(i) explain the purpose of cryptography

(ii) explain the purpose of encrypting data

(B) research historical uses of cryptography;

(i) research historical uses of cryptography

(C) review and explain simple cryptography methods such as shift cipher and substitution cipher;

(i) review simple cryptography methods

(ii) explain simple cryptography methods;

(D) define and explain public key encryption; and

(i) define public key encryption

(ii) explain public key encryption

(E) compare and contrast symmetric and asymmetric encryption.

(i) compare and contrast symmetric and asymmetric encryption

(16) Vulnerabilities, threats, and attacks. The student understands vulnerabilities, threats, and attacks. The student is expected to:

(A) explain how computer vulnerabilities leave systems open to cyberattacks;

(i) explain how computer vulnerabilities leave systems open to cyberattacks

(B) explain how users are the most common vehicle for compromising a system at the application level;

(i) explain how users are the most common vehicle for compromising a system at the application level

(C) define and describe vulnerability, payload, exploit, port scanning, and packet sniffing;

(i) define vulnerability

(ii) define payload

(iii) define exploit

(iv) define port scanning

(v) define packet sniffing

(vi) describe vulnerability

(vii) describe payload

(viii) describe exploit

(ix) describe port scanning

(x) describe packet sniffing

(D) identify internal threats to systems such as logic bombs and insider threats;

(i) identify internal threats to systems

(E) define and describe cyberattacks, including man-in-the-middle, distributed denial of service, spoofing, and back-door attacks;

(i) define cyberattacks, including man-in-the-middle attacks

(ii) define cyberattacks, including distributed denial of service attacks

(iii) define cyberattacks, including spoofing attacks

(iv) define cyberattacks, including back-door attacks

(v) describe cyberattacks, including man-in-the-middle attacks

(vi) describe cyberattacks, including distributed denial of service attacks

(vii) describe cyberattacks, including spoofing attacks

(viii) describe cyberattacks, including back-door attacks

(F) differentiate types of social engineering techniques such as phishing; web links in email, instant messaging, social media, and other online communication with malicious links; shoulder surfing; and dumpster diving; and

(i) differentiate types of social engineering techniques

(G) identify various types of application-specific attacks such as cross-site scripting and injection attacks.

(i) identify various types of application-specific attacks

(17) Vulnerabilities, threats, and attacks. The student evaluates the vulnerabilities of networks. The student is expected to:

(A) compare vulnerabilities associated with connecting devices to public and private networks;

(i) compare vulnerabilities associated with connecting devices to public and private networks

(B) explain device vulnerabilities and security solutions on networks such as supply chain security and counterfeit products;

(i) explain device vulnerabilities

(ii) explain security solutions on networks

(C) compare and contrast protocols such as HTTP versus HTTPS;

(i) compare and contrast protocols

(D) debate the broadcasting or hiding of a wireless service set identifier (SSID); and

(i) debate the broadcasting or hiding of a wireless service set identifier (SSID)

(E) research and discuss threats such as mandatory access control (MAC) spoofing and packet sniffing.

(i) research threats

(ii) discuss threats

(18) Vulnerabilities, threats, and attacks. The student analyzes threats to computer applications. The student is expected to:

(A) define application security;

(i) define application security

(B) identify methods of application security such as secure development policies and practices;

(i) identify methods of application security

(C) explain the purpose and function of vulnerability scanners;

(i) explain the purpose of vulnerability scanners

(ii) explain the function of vulnerability scanners

(D) explain how coding errors may create system vulnerabilities such as buffer overflows and lack of input validation; and

(i) explain how coding errors may create system vulnerabilities

(E) analyze the risks of distributing insecure programs.

(i) analyze the risks of distributing insecure programs

(19) Risk assessment. The student understands risk and how risk assessment and risk management defend against attacks. The student is expected to:

(A) define commonly used risk assessment terms, including risk, asset, and inventory;

(i) define commonly used risk assessment terms, including risk

(ii) define commonly used risk assessment terms, including asset

(iii) define commonly used risk assessment terms, including inventory

(B) identify risk management strategies, including acceptance, avoidance, transference, and mitigation; and

(i) identify risk management strategies, including acceptance

(ii) identify risk management strategies, including avoidance

(iii) identify risk management strategies, including transference

(iv) identify risk management strategies, including mitigation

(C) compare and contrast risks based on an industry accepted rubric or metric such as Risk Assessment Matrix.

(i) compare and contrast risks based on an industry accepted rubric or metric