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.

(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) [illegible]

(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)

(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

(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 (rio)0.5lcs (rio)0.5lcs 46 (rio)0.5ss(s 46 (rio)0.(d)-3.9 (e)-1 (s

(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;

(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. ogo t(o)2 pberio84.1 (us)3.8 (0.6 ((o81 (f)1.6 (0.6 (c(r)3.7 (y)5.9 p o)2.l5(o84.1 g(r)3.7 ak)2 pTw 0h(y)5.9 (.)2.on)-

(i) i the pripose orfy(o81 g(r)3.7 ak)1.9 phTw 0yy

(ii) i the pripose of 0.6 (ev)8.9 (cri)9.7 y pti

()

(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 attack0.002 TyTn ste(t)1.6 ( )0.5 bi exetre.9

((i) explain oc(o)8 mvutrervlxnera17

(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