Cybersecurity Capstone

Subject: Career and Technical Education
Grade: 11
Expectations: 61
Breakouts: 115

(a) Introduction.

1. Career and technical education instruction provides content aligned with challenging academic standards, industry relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and emerging foundations.
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 sensitive information. Cybersecurity professionals prevent, detect, and respond to minimize disruptions to governments, organizations, and individuals.
4. In the Cybersecurity Capstone course, students will develop the knowledge and skills needed to explore advanced concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will develop security policies to mitigate risks. The skills obtained in this course prepare students for additional study toward industry certification. A variety of courses are available to students interested in the cybersecurity field. Cybersecurity Capstone may serve as a culminating 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) communicate an understanding of ethical and legal responsibilities in relation to the field of cybersecurity.

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

(ii) communicate an understanding of legal responsibilities in relation to the field of cybersecurity

(2) Employability skills. The student identifies various employment opportunities in the cybersecurity field. The student is expected to:

(A) develop a personal career plan along with the education, job skills, and experience necessary to achieve career goals;

(i) develop a personal career plan along with the education, job skills, and experience necessary to achieve career goals

(B) develop a resume or a portfolio appropriate to a chosen career plan; and

(i) develop a resume or a portfolio appropriate to a chosen career plan

(C) demonstrate interview skills for successful job placement.

(i) demonstrate interview skills for successful job placement

(3) Ethics and laws. The student evaluates ethical and current legal standards, rights, and restrictions governing technology, technology systems, digital media and information technology, and the use of social media in the context of today's society. The student is expected to:

(A) analyze and apply to a scenario local, state, national, and international cybersecurity laws such as David's Law and Digital Millennium Copyright Act;

(i) analyze local cybersecurity laws

(ii) analyze state cybersecurity laws

(iii) analyze national cybersecurity laws

(iv) analyze international cybersecurity laws

(v) apply to a scenario local cybersecurity laws

(vi) apply to a scenario state cybersecurity laws

(vii) apply to a scenario national cybersecurity laws

(viii) apply to a scenario international cybersecurity laws

(B) evaluate noteworthy incidents or events regarding cybersecurity; and

(i) evaluate noteworthy incidents or events regarding cybersecurity

(C) evaluate compliance requirements such as Section 508 of the Rehabilitation Act of 1973, Family Educational Rights and Privacy Act of 1974 (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act (GLBA), and Cybersecurity Maturity Model Certification (CMMC).

(i) evaluate compliance requirements

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

(A) debate the relationship between privacy and security; and

(i) debate the relationship between privacy and security

(B) differentiate between ethical and unethical behavior when presented with various scenarios related to cybersecurity activities.

(i) differentiate between ethical and unethical behavior when presented with various scenarios related to cybersecurity activities

(5) Cybersecurity skills. The student simulates the process of penetration testing. The student is expected to:

(A) illustrate the phases of penetration testing, including plan, discover, attack, and report;

(i) illustrate the phases of penetration testing, including plan

(ii) illustrate the phases of penetration testing, including discover

(iii) illustrate the phases of penetration testing, including attack

(iv) illustrate the phases of penetration testing, including report

(B) design a plan to gain authorization for penetration testing;

(i) design a plan to gain authorization for penetration testing

(C) evaluate commonly used vulnerability scanning tools such as port scanning, packet sniffing, and password crackers;

(i) evaluate commonly used vulnerability scanning tools

(D) develop a list of exploits based on results of scanning tool reports; and

(i) develop a list of exploits based on results of scanning tool reports

(E) prioritize a list of mitigations based on results of scanning tool reports.

(i) prioritize a list of mitigations based on results of scanning tool reports

(6) Cybersecurity skills. The student understands common cryptographic methods. The student is expected to:

(A) evaluate symmetric and asymmetric algorithms such as substitution cipher, Advanced Encryption Standard (AES), Diffie-Hellman, and Rivest-Shamir-Adleman (RSA);

(i) evaluate symmetric algorithms

(ii) evaluate asymmetric algorithms

(B) interpret the purpose of hashing algorithms, including blockchain;

(i) interpret the purpose of hashing algorithms, including blockchain

(C) demonstrate password salting;

(i) demonstrate password salting

(D) explain and create a digital signature; and

(i) explain a digital signature

(ii) create a digital signature

(E) illustrate steganography.

(i) illustrate steganography

(7) Cybersecurity skills. The student understands the concept of system defense. The student is expected to:

(A) explain the purpose of establishing system baselines;

(i) explain the purpose of establishing system baselines

(B) evaluate the role of physical security;

(i) evaluate the role of physical security

(C) evaluate the functions of network security devices such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), intrusion detection prevention systems (IDPS), and security information and event management (SIEM) systems;

(i) evaluate the functions of network security devices

(D) analyze log files for anomalies; and

(i) analyze log files for anomalies

(E) develop a plan demonstrating the concept of defense in depth.

(i) develop a plan demonstrating the concept of defense in depth

(8) Cybersecurity skills. The student demonstrates an understanding of secure network design. The student is expected to:

(A) explain the benefits of network segmentation, including sandboxes, air gaps, and virtual local area networks (VLAN);

(i) explain the benefits of network segmentation, including sandboxes

(ii) explain the benefits of network segmentation, including air gaps

(iii) explain the benefits of network segmentation, including virtual local area networks (VLAN)

(B) investigate and discuss the role of software-managed networks, including virtualization and cloud architecture;

(i) investigate the role of software-managed networks, including virtualization

(ii) investigate the role of software-managed networks, including cloud architecture

(iii) discuss the role of software-managed networks, including virtualization

(iv) discuss the role of software-managed networks, including cloud architecture

(C) evaluate the role of honeypots and honeynets in networks; and

(i) evaluate the role of honeypots in networks

(ii) evaluate the role of honeynets in networks

(D) create an incoming and outgoing network policy for a firewall.

(i) create an incoming network policy for a firewall

(ii) create an outgoing network policy for a firewall

(9) Cybersecurity skills. The student integrates principles of digital forensics. The student is expected to:

(A) identify cyberattacks by their signatures, indicators, or patterns;

(i) identify cyberattacks by their signatures, indicators, or patterns

(B) explain proper data acquisition;

(i) explain proper data acquisition

(C) examine evidence from devices for suspicious activities; and

(i) examine evidence from devices for suspicious activities

(D) critique current cybercrime cases involving digital forensics.

(i) critique current cybercrime cases involving digital forensics

(10) Cybersecurity skills. The student explores expanding and emerging technology. The student is expected to:

(A) describe the concept of Security as a Service and the role of managed security service providers (MSSP);

(i) describe the concept of Security as a Service

(ii) describe the role of managed security service providers (MSSP)

(B) describe the integration of artificial intelligence and machine learning in cybersecurity;

(i) describe the integration of artificial intelligence in cybersecurity

(ii) describe the integration of machine learning in cybersecurity

(C) investigate impacts made by predictive analytics on cybersecurity; and

(i) investigate impacts made by predictive analytics on cybersecurity

(D) research and investigate other emerging trends such as augmented reality and quantum computing.

(i) research other emerging trends

(ii) investigate other emerging trends

(11) Cybersecurity skills. The student uses various operating system environments. The student is expected to:

(A) select and execute appropriate commands via the command line interface (CLI) such as ls, cd, pwd, cp, mv, chmod, ps, sudo, and passwd;

(i) select appropriate commands via the command line interface (CLI)

(ii) execute appropriate commands via the command line interface (CLI)

(B) describe the file system structure for multiple operating systems;

(i) describe the file system structure for multiple operating systems

(C) manipulate and edit files within the CLI; and

(i) manipulate files within the CLI

(ii) edit files within the CLI

(D) determine network status using the CLI with commands such as ping, ifconfig/ipconfig, traceroute/tracert, and netstat.

(i) determine network status using the CLI with commands

(12) Cybersecurity skills. The student clearly and effectively communicates technical information. The student is expected to:

(A) collaborate with others to create a technical report;

(i) collaborate with others to create a technical report

(B) create, review, and edit a report summarizing technical findings; and

(i) create a report summarizing technical findings

(ii) review a report summarizing technical findings

(iii) edit a report summarizing technical findings

(C) present technical information to a non-technical audience.

(i) present technical information to a non-technical audience

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

(A) differentiate types of attacks, including operating systems, software, hardware, network, physical, social engineering, and cryptographic;

(i) differentiate types of attacks, including operating systems

(ii) differentiate types of attacks, including software

(iii) differentiate types of attacks, including hardware

(iv) differentiate types of attacks, including network

(v) differentiate types of attacks, including physical

(vi) differentiate types of attacks, including social engineering

(vii) differentiate types of attacks, including cryptographic

(B) explain blended threats such as combinations of software, hardware, network, physical, social engineering, and cryptographic;

(i) explain blended threats

(C) discuss types of risk, including business, operational, security, and financial;

(i) discuss types of risk, including business

(ii) discuss types of risk, including operational

(iii) discuss types of risk, including security

(iv) discuss types of risk, including financial

(D) discuss risk response techniques, including accept, transfer, avoid, and mitigate;

(i) discuss risk response techniques, including accept

(ii) discuss risk response techniques, including transfer

(iii) discuss risk response techniques, including avoid

(iv) discuss risk response techniques, including mitigate

(E) develop a plan of preventative measures based on discovered vulnerabilities and the likelihood of a cyberattack;

(i) develop a plan of preventative measures based on discovered vulnerabilities

(ii) develop a plan of preventative measures based on the likelihood of a cyberattack

(F) identify and discuss common vulnerability disclosure websites;

(i) identify common vulnerability disclosure websites

(ii) discuss common vulnerability disclosure websites

(G) describe common web vulnerabilities such as cross-site scripting, buffer overflow, injection, spoofing, and denial of service;

(i) describe common web vulnerabilities

(H) describe common data destruction and media sanitation practices such as wiping, shredding, and degaussing; and

(i) describe common data destruction practices

(ii) describe common media sanitation practices

(I) develop an incident response plan for a given scenario or attack.

(i) develop an incident response plan for a given scenario or attack

(14) Risk assessment. The student understands risk management processes and concepts. The student is expected to:

(A) describe Zero Trust, least privilege, and various access control methods such as mandatory access control (MAC), role-based access control (RBAC), and discretionary access control (DAC);

(i) describe Zero Trust

(ii) describe least privilege

(iii) describe various access control methods

(B) develop and defend a plan for multi-factor access control using components such as biometric verification systems, key cards, tokens, and passwords; and

(i) develop a plan for multi-factor access control using components

(ii) defend a plan for multi-factor access control using components

(C) review and appraise a disaster recovery plan (DRP) that includes backups, redundancies, system dependencies, and alternate sites.

(i) review a disaster recovery plan (DRP) that includes backups, redundancies, system dependencies, and alternate sites

(ii) appraise a disaster recovery plan (DRP) that includes backups, redundancies, system dependencies, and alternate sites

(15) Risk assessment. The student investigates the role and effectiveness of environmental controls. The student is expected to:

(A) explain commonly used physical security controls, including lock types, fences, barricades, security doors, and mantraps; and

(i) explain commonly used physical security controls, including lock types

(ii) explain commonly used physical security controls, including fences

(iii) explain commonly used physical security controls, including barricades

(iv) explain commonly used physical security controls, including security doors

(v) explain commonly used physical security controls, including mantraps

(B) describe the role of embedded systems such as fire suppression; heating, ventilation, and air conditioning (HVAC) systems; security alarms; and video monitoring.

(i) describe the role of embedded systems