Ohio CTE

Information Technology Career Field: Cybersecurity

Business Operations/21st Century Skills: Learners apply principles of economics, business management, marketing, and employability in an entrepreneur, manager, and employee role to the leadership, planning, developing, and analyzing of business enterprises related to the career field. 1

Outcome 1.12 **Cyberhygeine: Apply digital information security principles to keep information secure.** 1.12.

3 Interpret security policies through job specific training and training updates. 1.12.3.

4 Apply secure password behavior. 1.12.4.

5 Apply physical and virtual situational awareness (e.g., clean desk policies, shoulder surfing, social engineering, tailgating). 1.12.5.

IT Fundamentals: Learners apply fundamental principles of IT, including the history of IT and its impact on society, common industry terms, systems theory, information storage and retrieval, database management, and computer hardware, software, and peripheral device configuration and installation. This base of knowledge and skills may be applied across the career field. 2

Outcome 2.1 **Security, Risks, and Safeguards: Describe the need for security and explain security risks and security safeguards.** 2.1.

1 Explain the need for confidentiality, integrity, and availability (CIA) of information. 2.1.1.

2 Describe authentication, authorization, and auditing. 2.1.2.

3 Describe multilevel security. 2.1.3.

5 Describe major threats to computer systems (e.g., insider threats, viruses, worms, spyware, ransomware, spoofing, hacking, social engineering, phishing). 2.1.5.

10 Describe computer forensics, its importance in information security and cybersecurity, and its relevance to law enforcement. 2.1.10.

11 Identify the need for personal security in digital information and describe how personal information can be safeguarded. 2.1.11.

Outcome 2.4 **Emerging Technologies: Identify trending technologies, their fundamental architecture, and their value in the marketplace.** 2.4.

1 Investigate the scope and the impact of mobile computing environments on society. 2.4.1.

2 Describe the differences, advantages, and limitations of cloud computing (e.g., public cloud, private cloud, hybrid cloud) and on-premises computing. 2.4.2.

4 Describe emerging technologies (e.g., Bring your Own Device [BYOD], Services Virtualization, Augmented Reality [AR], SMART Devices, Additive Manufacturing [3D Printing]). 2.4.4.

Information Security: Learners apply principles of information security to implement and maintain security compliance and network security. Learners select components and mechanisms required for a multilayer defense structure and evaluate and minimize security risks to wired and wireless networks and devices. 3

Outcome 3.1 **Components of Information Security: Describe the components associated with information security systems.** 3.1.

1 Differentiate between authentication and authorization. 3.1.1.

2 Compare authentication techniques (e.g. single factor, multifactor, passwords, biometrics, certificates, Radio Frequency Identification [RFID] cards). 3.1.2.

4 Describe Virtual Private Networks (VPNs) using tunneling protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Secure Socket Tunneling Protocol [SSTP], Point-to-Point Tunneling Protocol [PPTP] and encrypting techniques). 3.1.4.

Outcome 3.2 **Implement and maintain general security compliance.: Describe the components associated with information security systems.** 3.2.

1 Identify and implement data and application security. 3.2.1.

8 Identify the need for disaster recovery policies and procedures. 3.2.8.

Outcome 3.3 **Network Security: Implement and maintain network security.** 3.3.

1 Describe network security policies (e.g., acceptable use policy). 3.3.1.

5 Assess risks based on vulnerability of the organization, likelihood of risk, and impact on the organization. 3.3.5.

6 Describe the functions and uses of patch management. 3.3.6.

Outcome 3.4 **Multilayer Defense Structure: Explain information technology mechanisms as they apply to a multilayer defense structure.** 3.4.

4 Identify the components of human security (e.g., social engineering) and techniques to mitigate human security threats (e.g., policies, procedures, training). 3.4.4.

Outcome 3.5 **Wireless Security: Implement secure wireless networks.** 3.5.

1 Describe wireless security risks (e.g., unauthorized access) and how to mitigate them. 3.5.1.

5 Describe security practices and policies for personal devices. 3.5.5.

6 Implement and test the security of a wireless network. 3.5.6.

Infrastructure Systems: Learners apply principles of networking and infrastructure related to the installation, administration, and maintenance of computer networks and components. Knowledge and skills may be applied to network connectivity, cabling, protocols, architecture, classification, topologies, operating systems, Open Systems Interconnection (OSI) standards, data encoding, Quality of Service (QoS), Internet Protocol (IP) addressing, and wide area network (WAN) design. 4

Outcome 4.1 **Network Infrastructure: Build a multinode network.** 4.1.

1 Determine the basic point-to-point (PTP) and point-to-multipoint (PTMP) network topologies (e.g., star, ring, tree, mesh, hybrid) and identify broadband and baseband (e.g., Ethernet) transmission methods and standards. 4.1.1.

4 Identify standard and emerging network technologies (e.g., broadband, satellite, optic, cellular, Local-Area Network (LAN) and WiFi). 4.1.4.

6 Configure and build a network. (e.g., server, switch, router) 4.1.6.

Outcome 4.2 **Open Systems Interconnection: Describe the Open Systems Interconnection (OSI) standard (International Organization for Standardization [ISO] Standard 7498).** 4.2.

3 Compare the seven layers of the Open Systems Interconnection stack to the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) stack. 4.2.3.

5 Describe actions to be performed at each of the Open Systems Interconnection physical layers. 4.2.5.

Outcome 4.3 **Network Media Select, assemble, terminate, and test media.** 4.3.

1 Identify the criteria used in selecting media (e.g., physical properties, transmission technologies, transmission span, bandwidth, topology, security, noise immunity, installation considerations, cost). 4.3.1.

2 Differentiate between media types (e.g., coaxial, twisted pair, fiber optic) and interfaces. 4.3.2.

3 Compare media categories (e.g., single mode, multimode, CAT5, CAT5E, CAT6+). 4.3.3.

4 Describe types of media connectors (e.g., Bayonet Neill-Concelman [BNC], Registered Jack [RJ]-45, LC, ST) and grounding techniques. 4.3.4.

6 Identify the advantages and disadvantages of cabling systems. 4.3.6.

Outcome 4.4 **Wireless Communications: Explain wireless communications.** 4.4.

1 Compare wireless standards in common use (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.11, Cellular, Bluetooth, Worldwide Interoperability for Microwave Access [WiMAX], Radio Frequency Identification [RFID], Near Field Communication [NFC]). 4.4.1.

Outcome 4.5 **Wireless Network Solutions: Explain wireless communications.** 4.5.

3 Describe the Service Set Identifier (SSID) as used in wireless communications. 4.5.3.

4 Select and install access points, wireless Network Interface Cards (NICs), antennas, and other hardware and software components to provide a wireless networking solution as determined by a site and customer survey. 4.5.4.

6 Secure the wireless network. 4.5.6.

Outcome 4.7 **Transmission Control Protocol/Internet Protocol (TCP/IP): Describe IP addressing schemes and create subnet masks.** 4.7.

1 Explain Fully Qualified Domain Names (FQDNs) and how they are used. 4.7.1.

2 Explain the IP addressing scheme and how it is used. 4.7.2.

3 Identify Class A, B, and C reserved (i.e., private) address ranges and why they are used. 4.7.3.

4 Identify the class of network to which a given address belongs. 4.7.4.

Cybersecurity: Learners apply principles of cybersecurity to secure and defend information technology systems, selection and implementation of methods and tools to secure physical and digital assets, mange threats, deploy countermeasures, and establish strategies to protect business information using risk and incident management. 9

Outcome 9.1 **Cybersecurity: Examine and employ principles of cybersecurity.** 9.1.

1 Identify the goals, objectives and purposes of cybersecurity. 9.1.1.

2 Describe the concepts of malware attack vectors. 9.1.2.

5 Identify types of controls (e.g., Deterrent, Preventive, Detective, Compensating, Technical, and Administrative). 9.1.5.

Outcome 9.3 **Application Development Security: Develop and maintain application security.** 9.3.

1 Identify application vulnerabilities (e.g., Cross-site scripting, SQL injection, LDAP injection, XML injection, Directory traversal/command injection, Buffer overflow, Integer overflow, Zero-day, Cookies and attachments, Locally Shared Objects (LSOs), Flash cookies, Malicious add-ons, Session hijacking, Header manipulation, Arbitrary code execution/remote code execution). 9.3.1.

6 Differentiate between Server-side vs. client-side validation. 9.3.6.

Outcome 9.5 **Threat Management: Mitigate common threats.** 9.5.

1 Describe, locate, and mitigate security threats (e.g., Adware, Viruses, Spyware, Trojan, Rootkits, Logic bomb, Botnets, Ransomware, Polymorphic malware). 9.5.1.

2 Describe and discover vulnerabilities to and mitigate network attacks. (e.g., Man-in-the-middle, DDoS, DoS, Replay, Smurf attack, Spoofing, Spam, Phishing, Spim, Spit and other attacks). 9.5.2.

4 Describe, appraise for, and mitigate Social Engineering attacks (e.g., Shoulder surfing, Dumpster diving, Tailgating, Impersonation, Hoaxes, Phishing, Spear Phishing, Whaling, Vishing, Principles, URL hijacking, Watering Hole). 9.5.4.

Outcome 9.7 **Digital Forensics: Capture and analyze information using digital tools.** 9.7.

1 Recognize digital reconnaissance techniques (e.g., packet capture, OS fingerprinting, topology discovery, DNS harvesting). 9.7.1.

4 Collect digital evidence according to established policies and protocols (e.g., system image, packet captures). 9.7.4.

5 Maintain chain of custody on evidence. 9.7.5.

Outcome 9.8 **Countermeasures: Use countermeasures to monitor systems and reduce risk.** 9.8.

2 Differentiate between detection controls and prevention controls (e.g., IDS vs. IPS, Camera vs. guard). 9.8.2.

3 Use discovery tools and utilities to identify threats (e.g., Protocol analyzer, Vulnerability scanner, Honeypots, Honeynets, Port scanner). 9.8.3.

9 Interpret alarms and alert trends. 9.8.9.

10 Apply Incident response procedures (e.g., Preparation, Incident identification, Escalation and notification, Mitigation steps, Lessons learned, Reporting, Recovery procedures, First responder, Incident isolation, Quarantine, Device removal, Data breach). 9.8.10

11 Differentiate between types of Penetration testing (e.g., Black box, White box, Gray box). 9.8.11.