Ohio CTE

Information Technology Career Field: Cybersecurity Defense and Reinforcement

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 **Cyber Hygiene: Apply digital information security principles to keep information secure.** 1.12.

2 Differentiate between appropriate and inappropriate information. 1.12.2.

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.

2 Describe authentication, authorization, and auditing. 2.1.2.

4 Identify security risks and describe associated safeguards and methodologies (e.g., auditing). 2.1.4.

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.

12 Practice information security per job requirements. 2.1.12.

13 Describe privacy security compliance on systems (e.g., Health Insurance Portability and Accountability Act [HIPAA], Payment Card Industry [PCI], Sarbanes Oxley Act [SOX], Americans with Disabilities Act [ADA], General Data Protection Regulation [GDPR], European Union Data Protection Regulation [EUDPR]). 2.1.13.

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.

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

4 Provide user authentication (e.g., assign and reset user accounts and passwords). 3.2.4

5 Install, test, implement, and update virus and malware detection and protection software. 3.2.5

6 Identify sources of virus and malware infection and remove viruses and malware. 3.2.6

7 Provide documentation, training, and support to users on established security procedures. 3.2.7

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

7 Train users in network security procedures. 3.3.7

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

2 Analyze system log files to identify security risks. 3.4.2

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

2 Compare methods of increasing the security of wireless networks and devices (e.g., Media Access Control [MAC] address filtering, Wi-Fi Protected Access [WPA], 802.1x, Remote Authentication Dial In User Service [RADIUS]). 3.5.2

3 Research security enhancements provided by Institute of Electrical and Electronics Engineers (IEEE). 3.5.3

4 Describe practices and policies for preventing and detecting installation of rogue networks. 3.5.4

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

Outcome 4.5 **Wireless Network Solutions: Design and implement wireless network solutions.** 4.5.

6 Secure the wireless network. 4.5.6.

Outcome 4.6 **Network Protocols: Compare network protocols.** 4.6.

2 Identify the advantages of protocols (e.g., Domain Name System [DNS], File Transfer Protocol [FTP], Hypertext Transfer Protocol [HTTP], Telecommunications Network [Telnet], Remote Desktop Protocol [RDP]], Secure Shell [SSH]) and associated port numbers. 4.6.2

7 Describe a Virtual Private Network (VPN) and identify associated protocols (e.g., Layer 2 Tunneling Protocol [L2TP], Point-to-Point Tunneling Protocol [PPTP]). 4.6.7.

Interconnection (OSI) standards, data encoding, Quality of Service (QoS), Internet Protocol (IP) addressing, and wide area network (WAN) design. 4

Outcome 4.11 **Cloud Computing: Implement a hypervisor.** 4.11.

2 Provision cloud services (e.g., Software as a Service [SaaS], Platform as a Service [PaaS], Infrastructure as a Service [IaaS], Security as a Service). 4.11.2

Outcome 4.13 **Disaster Recovery: Recommend disaster recovery and business continuity plans.** 4.13.

1 Differentiate between disaster recovery and business continuity. 4.13.1.

2 Identify common backup devices. 4.13.2.

3 Identify the criteria for selecting a backup system. 4.13.3.

4 Establish a process for archiving files. 4.13.4.

5 Develop a disaster recovery plan. 4.13.5.

Cyber Security: 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 **Cyber Security: Examine and employ principles of cyber security.** 9.1.

1 Identify the goals, objectives and purposes of Cyber Security. 9.1.1

2 Describe the concepts of malware attack vectors. 9.1.2

3 Maintain data security using data labeling, handling and, disposal as prescribed by policy and law. 9.1.3

4 Mitigate threats by remaining abreast of industry information. 9.1.4

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

Outcome 9.2 **Access Control and Asset Security: Apply identification (ID), authorization, and physical asset security.** 9.2.

1. Perform authorization control (e.g., least privilege, separation of duties, mandatory access, discretionary access, rule-based access control, role-based access control, time of day restrictions, location distractions). 9.2.1
2. Implement authentication techniques (e.g., Tokens, Common access card, Smart card, Multifactor authentication, Single sign-on, Biometrics, Personal identification verification card, Username, Federation, Transitive trust/authentication). 9.2.2
3. Use authentication factors (e.g., Something you are, Something you have, Something you know). 9.2.3
4. Mitigate security implications of third party connectivity and access. 9.2.4
5. Implement Data Loss Prevention (DLP). 9.2.5
6. Implement perimeter security (e.g., Fencing, Proximity readers, Access list, Proper lighting, Mantraps, Video Surveillance, Signs, Guards, Barricades, Biometrics, Protected distribution (cabling), Alarms, Motion detection). 9.2.6
7. Inventory devices. 9.2.7

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.
2. Mitigate application attacks (e.g., SANS, OWASP). 9.3.2
3. Implement secure coding concepts (e.g., Error and exception handling, Input validation, Cross-site scripting prevention, Cross-site Request Forgery, (XSRF) prevention, OWASP). 9.3.3
4. Implement secure application configuration (e.g., Application hardening, Application patch management). 9.3.4
5. Discover and mitigate common database vulnerabilities and attacks. 9.3.5
6. Differentiate between Server-side vs. client-side validation. 9.3.6

Outcome 9.4 **Setup a Secure Network: Setup and maintain network security.** 9.4.

1. Setup and maintain secure roles and system management techniques (e.g., password, group, and user privilege policies and monitoring). 9.4.1
2. Secure use of network Protocols (e.g., IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS, HTTPS, SCP, ICMP). 9.4.2
3. Apply principles of IPv4 and IPv6 securely. 9.4.3
4. Apply wireless security configurations (e.g., Disable SSID broadcast, TKIP, CCMP, Antenna placement, Power level controls). 9.4.4
5. Manage PKI and certificates (Transport encryption, Non-repudiation, Hashing, Key escrow, Steganography, Digital signatures). 9.4.5
6. Use of algorithms/protocols with transport encryption (e.g., SSL, TLS, IPSec, SSH, HTTPS). 9.4.6
7. Install and configure network devices (firewalls, switches, load balancers, proxies, web security gateways, VPN concentrators). 9.4.7
8. Install and configure network security devices. (Protocol analyzers, Spam filter, UTM security appliances, URL filter, Content inspection, Malware inspection). 9.4.8
9. Implement port security. 9.4.9
10. Monitor and manage network Unified Threat Management. 9.4.10
11. Mitigate network threats (e.g., Flood guards, Loop protection, Implicit deny, Network separation, Log analysis, Unified threat management, peripheral and removable media). 9.4.11
12. Apply the principles of secure Network Design (e.g., DMZ, Subnetting, NAT/PAT, Remote access, Telephony, Virtualization). 9.4.12

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.
3. Configure defenses for Password attacks (e.g., Brute Force, Dictionary attacks, Hybrid, Birthday attacks, Rainbow tables). 9.5.3
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 9.6 **Cyber Security Law: Adhere to cyber security laws.** 9.6.

1 Adhere to licensing and intellectual property laws (e.g., copyright, trademark, digital-rights management). 9.6.1

2 Adhere to regulatory and industry standards (e.g., PCIDSS, PADSS). 9.6.2

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.

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

1 Design and implement network segmentation. 9.8.1

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

4 Create, edit and use roles and system management tools. 9.8.4

5 Implement endpoint security. 9.8.5

6 Implement Access Control Lists (ACL). 9.8.6

7 Deploy a server hardening plan. 9.8.7

8 Implement a Network Access Control (NAC) plan. 9.8.8

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

Outcome 9.9 **Disaster Recovery and Business Continuity: Apply fundamentals of disaster recovery and business continuity.** 9.9.

1. Describe the concepts of Risk Management (e.g., Business continuity concepts, Business impact analysis, Identification of critical systems and components, Removing single points of failure). 9.9.1
2. Describe the concepts of Risk assessment (e.g., Disaster recovery plan, IT contingency planning - Succession planning, Redundancy). 9.9.2
3. Describe and plan Fault tolerance (e.g., Hardware, RAID, Clustering, Load balancing, Disaster recovery concepts, Backup plans/policies, Backup execution/frequency). 9.9.3

Outcome 9.10 **Risk Management: Apply concepts of risk management.** 9.10.

1. Enforce concepts related to threat vectors and probability/threat likelihood. 9.10.1
2. Identify concepts of risk calculation (Likelihood, ALE, Impact, SLE, ARO, MTTR, MTTF, MTBF). 9.10.2
3. Implement Governance, risk management and Compliance Management processes (risk mitigation, govern compliance). 9.10.3