Virginia CTE

Cybersecurity Fundamentals (6302)

Exploring Cybersecurity Fundamentals CF.1

1. Describe cybersecurity. CF.1.1
2. Describe the critical factors of information assurance. CF.1.2
3. Define vulnerability and risk. CF.1.3
4. Explain why organizations need to manage risk. CF.1.4
5. Identify the concepts of cybersecurity risk management. CF.1.5
6. Describe cybersecurity threats to an organization. CF.1.6
7. Describe national and industry standards and regulations that relate to cybersecurity. CF.1.7
8. Describe the cyberattack surface of various organizations. CF.1.8
9. Analyze risks affecting critical infrastructure. CF.1.9

Examining Computer Networks as a Foundational Element of Cybersecurity CF.2

1. Describe computer components. CF.2.1
2. Describe a network. CF.2.2
3. Describe a wired network. CF.2.3
4. Describe a wireless network. CF.2.4
5. (Optional) Compare wired and wireless networks. CF.2.5
6. Compare networking conceptual models. CF.2.6
7. Discuss services and potential vulnerabilities. CF.2.7
8. Differentiate between network types. CF.2.8
9. Describe the concept of the Internet as a network of connected systems. CF.2.9
10. Identify networking protocols. CF.2.10

Understanding Cyber Threats and Vulnerabilities CF.3	1	**Differentiate between a cyber threat and a vulnerability.** CF.3.1
	2	**Describe types of cyber threats.** CF.3.2
	3	**Analyze types of current cyber threats.** CF.3.3
	4	**Describe the concept of malware and the techniques to guard against it.** CF.3.4
	5	**Identify the perpetrators of different types of malicious hacking.** CF.3.5
	6	**Describe the characteristics of vulnerabilities.** CF.3.6
	7	**Identify the prevention of and protections against cyber threats.** CF.3.7
	8	**(Optional) Identify the cyber risks associated with bring your own device (BYOD) opportunities on computer networks.** CF.3.8
Exploring Ethics as it Relates to Cybersecurity CF.4	1	**Differentiate between ethics and laws.** CF.4.1
	2	**Distinguish among types of ethical concerns.** CF.4.2
	3	**Define cyberbullying.** CF.4.3
	4	**Identify actions that constitute cyberbullying.** CF.4.4
	5	**(Optional) Identify possible warning signs of someone being cyberbullied.** CF.4.5
	6	**(Optional) Demonstrate net etiquette (i.e., netiquette) as it relates to cybersecurity.** CF.4.6
	7	**Identify laws applicable to cybersecurity.** CF.4.7
Exploring Data Privacy CF.5	1	**Explain the concept of "personally identifiable information."** CF.5.1
	2	**Explain why personal data is valuable to both an individual and to organizations (e.g., governments, businesses) that collect it, analyze it, and make decisions based on it.** CF.5.2
	3	**Explain the techniques used to collect personal data through social media, web tracking, and mobile devices.** CF.5.3
	4	**Identify ways to control and protect personal data.** CF.5.4
	5	**Analyze the social and legal significance of the ongoing collection of personal digital information.** CF.5.5
Examining Data Security as it Relates to Cybersecurity CF.6	1	**Distinguish between data, information, and knowledge.** CF.6.1
	2	**Identify the most common ways data is collected.** CF.6.2

	3 Identify the most common ways data can be stored. CF.6.3
	4 Explain the difference between data at rest, data in transit, and data being processed. CF.6.4
	5 Identify the most common ways data is used. CF.6.5
	6 Discuss how data can be compromised, corrupted, or lost. CF.6.6
	7 Explain how businesses and individuals can protect themselves against threats to their data. CF.6.7
Securing Operating Systems CF.7	1 Define the function of a computer operating system. CF.7.1
	2 (Optional) Identify the components of an operating system. CF.7.2
	3 List types of operating systems. CF.7.3
	4 Identify examples of widely used desktop and server operating systems. CF.7.4
	5 Evaluate the potential vulnerabilities, threats, and common exploits to an operating system. CF.7.5
	6 Identify best practices for protecting operating systems. CF.7.6
	7 Evaluate critical operating system security parameters. CF.7.7
	8 (Optional) Describe security and auditing logs. CF.7.8
	9 (Optional) Describe the role of a system backup. CF.7.9
	10 Define virtualization technology. CF.7.10
	11 (Optional) Identify advantages and disadvantages of using virtual machines. CF.7.11
Programming as a Component of Cybersecurity CF.8	1 Identify representation of data at lowest levels. CF.8.1
	2 Define programming in the context of cybersecurity. CF.8.2
	3 Differentiate between computer programming languages. CF.8.3
	4 (Optional) Describe Python. CF.8.4
	5 (Optional) Demonstrate Linux. CF.8.5
	6 (Optional) Evaluate common programming flaws that lead to vulnerabilities. CF.8.6
	7 Identify best practices in secure coding and design. CF.8.7

Exploring Cybersecurity Implications for Current and Emerging Technologies CF.9	1	**Identify ubiquitous computing.** CF.9.1
	2	**Description security and privacy implications of ubiquitous computing.** CF.9.2
Exploring Cybersecurity Careers CF.10	1	**Research career opportunities for cybersecurity professionals.** CF.10.1
	2	**Examine the Career Clusters affected by current and emerging technology.** CF.10.2
	3	**Identify the educational pathways for emerging cybersecurity professionals.** CF.10.3
	4	**Identify career paths and job titles within the cybersecurity and/or cyber forensics industry and Career Clusters.** CF.10.4
	5	**Research the cyber threats and security measures related to career pathways.** CF.10.5
Preparing for Industry Certification CF.11	1	**Identify testing skills and strategies for a certification examination.** CF.11.1
	2	**Describe the process and requirements for obtaining industry certifications related to the Cybersecurity Fundamentals course.** CF.11.2
	3	**Demonstrate the ability to complete selected practice examinations.** CF.11.3
	4	**Successfully complete an industry certification examination representative of skills learned in this course.** CF.11.4