

FBLA HS Cybersecurity*

Security Fundamentals (15 test items)

1. Describe Confidentiality, Integrity, and Availability
2. Describe measures for establishing digital trust (e.g., identity proofing, non-repudiation, attestation)
3. Explain the concepts of authentication, authorization, and accounting
4. Provide examples of Zero Trust
5. Describe examples of deception and disruption technology for defending against attackers (e.g., honeypots, honeynets, honeyfiles)
6. Explain how binary, hexadecimal, and decimal are used in cryptography
7. Explain the purpose of least privilege principles

Cyber Threats and Vulnerabilities (20 test items)

1. Describe web and software sources of security vulnerabilities (e.g., injections, overflows, jailbreaking, race conditions)
2. Discuss attributes of threat actors and their goals (e.g., internal and external threats, financial gain, espionage, data theft)
3. Describe types of viruses
4. Discuss types of security vulnerabilities (e.g., backdoors, zero-days, unpatched software)
5. Discuss social engineering scams and attacks (e.g., phishing, phone scams, email scams)
6. Describe the purpose, methods, and mechanics of a DDoS attack
7. Describe the characteristics of types of malware (e.g., viruses, Trojans, worm, logic bombs)
8. Describe cryptographic attacks (e.g., downgrades, collisions, birthday attacks)
9. Discuss vulnerabilities of wireless networks

* Sources: These learning outcomes are based on content from the Cybersecurity Curricula 2017, Security+ Certification Exam Objectives, and K-12 Cybersecurity Learning Standards.

Security and Design (20 test items)

1. Explain how using cloud infrastructure affects system security
2. Discuss the security implications of microservice architecture (e.g., more attack surfaces, authentication, increased complexity)
3. Differentiate between logical and physical segmentation
4. Explain how containerization and virtualization can increase security
5. Describe security risks and challenges associated with the Internet of Things
6. Describe the concepts of backups, RAID, and UPS
7. Identify examples of the CIA triad in network design (e.g., UPS, encryption, data integrity)
8. Explain the role of testing in building secure cyber architecture

Network and Data Security (15 test items)

1. Describe the purpose of cryptography
2. Differentiate between public and private key cryptography
3. Discuss shift ciphers, Caesar ciphers, and substitution ciphers
4. Describe the three states of data
5. Describe the importance and use of access control models (e.g., MAC, DAC, RBAC)
6. Discuss authentication and authorization of network resources (e.g., multifactor, certificates, tokens)
7. Describe how blockchains and hashing can be used for authentication and data integrity

Security Operations and Management (10 test items)

1. Describe common security policies (e.g., acceptable use, information security, business continuity, disaster recovery)
2. Discuss elements of disaster prevention and recovery plans
3. Describe types of firewalls (e.g., network-based, NGFW, WAF)
4. Explain the use of firewall access lists and rules to increase security
5. Describe best practices for company messaging, email, and data security
6. Describe the impact of change management on security

Security Protocols and Threat Mitigation (20 test items)

1. Provide examples of secure protocols (e.g., SSH, HTTPS, TLS, WPA2)
2. Describe the purpose of intrusion prevention and detection systems
3. Describe policies and practices to prevent viruses, phishing and email scams
4. Explain methods of obfuscation (e.g., tokenization, data masking, steganography)
5. Describe how strong passwords increase security
6. Describe the purpose of digital certificates and Certificate Authorities (CAs)
7. Describe the importance of patches, updates, and version control for security
8. Explain the use of pen testing for increasing security

References

Adelaide University. *Cyber security basics: Exploring the fundamentals of cyber security*.

<https://online.adelaide.edu.au/blog/cyber-security-fundamentals>

Association for Computing Machinery. *Cybersecurity Curricula 2017*.

https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

Codecademy. *Introduction to cybersecurity*. <https://www.codecademy.com/learn/introduction-to-cybersecurity>

CompTIA. *Security+ Certification Exam Objectives*.

<https://assets.ctfassets.net/82ripq7fjls2/6TYWUym0Nudqa8nGEnegjG/0f9b974d3b1837fe85ab8e6553f4d623/CompTIA-Security-Plus-SY0-701-Exam-Objectives.pdf>

Cybersecurity Guide. *Mastering the basics: A comprehensive guide to cybersecurity 101 for the digital age*. <https://cybersecurityguide.org/resources/cybersecurity-101/>

The Academic Initiative of the Cyber Innovation Center. *K-12 Cybersecurity Learning Standards*.

https://cyber.org/sites/default/files/2021-10/K-12%20Cybersecurity%20Learning%20Standards_1.0.pdf