FBLA Cybersecurity Sample Questions

Disclaimer: *These are sample test questions of what a competitor will find in this competition. To view the official study guide, with the knowledge area and objective list, visit the guidelines on the Competitive Events page of the national website at www.fbla.org.*

Security Fundamentals

1. Which of the following best defines cybersecurity?
   a) The use of firewalls to block all incoming traffic
   b) Protecting systems, networks, and programs from digital attacks
   c) Removing viruses from computers after infection
   d) Encrypting all data regardless of need

2. Which principle of the CIA Triad ensures that information is only accessible to authorized users?
   a) Integrity
   b) Availability
   c) Confidentiality
   d) Authenticity

3. A key reason for implementing access control is to:
   a) Increase internet speed
   b) Restrict unauthorized access to data and systems
   c) Install antivirus software
   d) Enable unlimited data sharing

4. Which is an example of a physical security control?
   a) Firewall rules
   b) Password complexity
   c) Security guards and locked doors
   d) Data encryption

5. Multi-factor authentication improves security by:
   a) Replacing all passwords with PINs
   b) Requiring multiple forms of verification
   c) Limiting network access times
   d) Encrypting stored passwords

6. Which of the following is NOT a common element of cybersecurity policy?
   a) Incident response procedures
   b) Acceptable use guidelines
   c) Disaster recovery plan
   d) Sales quotas

7. The process of ensuring that data has not been altered is called:
   a) Confidentiality
   b) Non-repudiation
   c) Integrity
   d) Availability

8. Which is an example of a technical security control?
   a) Employee training
   b) Antivirus software
   c) Security awareness posters
   d) Locked filing cabinets

Cyber Threats and Vulnerabilities

9. Which type of malware demands payment to restore access to data?
   a) Spyware
   b) Trojan horse
   c) Ransomware
   d) Worm

10. A phishing attack is designed to:
    a) Overload a system with traffic
    b) Trick users into revealing sensitive information
    c) Destroy hardware components
    d) Corrupt system files

11. Which is an example of a zero-day vulnerability?
    a) A known bug that has been patched
    b) A newly discovered software flaw without a fix
    c) Outdated security software
    d) Weak password usage

12. Which type of attack floods a system with traffic to make it unavailable?
    a) SQL injection
    b) Brute force
    c) Distributed Denial of Service (DDoS)
    d) Phishing

13. Social engineering exploits:
    a) Human behavior and trust
    b) Software vulnerabilities
    c) Network protocols
    d) Hardware limitations

14. An insider threat is best described as:
    a) A hacker from a foreign country
    b) A malicious or negligent action by someone within the organization
    c) A virus from the internet
    d) An accidental data breach from a customer

15. Which attack inserts malicious code into a website's database through user input fields?
    a) DDoS attack
    b) Cross-site scripting (XSS)
    c) SQL injection
    d) Keylogging

Disclaimer: These are sample test questions of what a competitor will find in this competition. To view the official study guide, with the knowledge area and objective list, visit the guidelines on the Competitive Events page of the national website at www.fbla.org.

16. Spyware is designed to:
    a) Monitor user activity without consent
    b) Encrypt files until payment is made
    c) Erase the hard drive
    d) Improve system performance

17. Which is the most common cause of security breaches?
    a) Natural disasters
    b) Human error
    c) Hardware malfunction
    d) Solar flares

18. A vulnerability scan is used to:
    a) Create strong passwords
    b) Identify weaknesses in systems and networks
    c) Remove malware
    d) Configure firewall rules

Security and Design

19. Security by design means:
    a) Adding security features after development
    b) Building security into every stage of system development
    c) Ignoring security until testing
    d) Using only physical controls

20. The principle of least privilege states that:
    a) Users should have access only to what they need to perform their job
    b) All users should have admin rights
    c) Guests should have access to most resources
    d) Security should be minimal to improve speed

21. Threat modeling is used to:
    a) Identify and prioritize potential security threats during design
    b) Create a network map
    c) Install antivirus software
    d) Develop marketing strategies

22. A secure software development lifecycle (SDLC) focuses on:
    a) Reducing project costs
    b) Integrating security measures throughout development
    c) Limiting documentation
    d) Avoiding user testing

23. Which is NOT a secure coding practice?
    a) Input validation
    b) Hard-coding passwords
    c) Error handling
    d) Code review

Disclaimer: These are sample test questions of what a competitor will find in this competition. To view the official study guide, with the knowledge area and objective list, visit the guidelines on the Competitive Events page of the national website at www.fbla.org.

24. What is the primary benefit of code reviews for security?
    a) Increasing development time
    b) Detecting vulnerabilities before deployment
    c) Reducing documentation requirements
    d) Allowing unauthorized code changes

25. Which security measure is most effective against SQL injection?
    a) Data encryption
    b) Input validation and parameterized queries
    c) Antivirus software
    d) Password complexity rules

26. What is a sandbox in cybersecurity?
    a) A physical space for training
    b) An isolated environment for testing untrusted code
    c) A cloud-based backup system
    d) A network firewall

27. Which of the following best describes secure configuration management?
    a) Maintaining consistent, approved settings for systems and devices
    b) Allowing each user to configure systems as they wish
    c) Avoiding updates for stability
    d) Using default manufacturer settings

28. Security requirements in system design should be:
    a) Considered from the start of the project
    b) Added after testing
    c) Optional for speed
    d) Ignored unless mandated by law

Network and Data Security

29. Which device filters network traffic based on predefined security rules?
    a) Router
    b) Switch
    c) Firewall
    d) Modem

30. Data encryption is primarily used to:
    a) Speed up network performance
    b) Prevent unauthorized access to information
    c) Back up data automatically
    d) Delete unnecessary files

31. Which protocol is used for secure communication over the internet?
    a) HTTP
    b) FTP
    c) HTTPS
    d) SMTP

Disclaimer: These are sample test questions of what a competitor will find in this competition. To view the official study guide, with the knowledge area and objective list, visit the guidelines on the Competitive Events page of the national website at www.fbla.org.

32. A Virtual Private Network (VPN) provides security by:
    a) Physically disconnecting from the internet
    b) Encrypting network traffic between endpoints
    c) Installing antivirus software
    d) Blocking all downloads

33. Which type of firewall monitors the state of active connections?
    a) Packet-filtering firewall
    b) Stateful inspection firewall
    c) Circuit-level gateway
    d) Application-layer firewall

34. Data loss prevention (DLP) tools are used to:
    a) Prevent unauthorized transfer of sensitive data
    b) Speed up network connections
    c) Block all internet access
    d) Create backups

35. Which wireless security protocol is most secure for home networks?
    a) WEP
    b) WPA2/WPA3
    c) Open network
    d) WPA with TKIP only

Security Operations and Management

36. An incident response plan should:
    a) Be developed after a breach occurs
    b) Outline steps for detecting, responding to, and recovering from incidents
    c) Focus only on physical security
    d) Be used only by management

37. Which is the first step in the incident response process?
    a) Containment
    b) Detection and identification
    c) Eradication
    d) Recovery

38. Security awareness training helps employees:
    a) Understand and follow security policies
    b) Avoid using technology altogether
    c) Replace IT staff
    d) Identify technical vulnerabilities in code

39. A business continuity plan ensures:
    a) Operations can continue during and after a disruption
    b) All employees take vacations
    c) Only security staff remain during incidents
    d) Backups are optional

40. Which role is responsible for managing overall information security within an organization?
    a) CIO
    b) CISO
    c) CTO
    d) CEO

Security Protocols and Threat Mitigation

41. Which is an example of strong password practice?
    a) Using your birthdate
    b) Creating a long password with letters, numbers, and symbols
    c) Using “password123”
    d) Reusing the same password for all accounts

42. Which technology uses a secret key for both encryption and decryption?
    a) Symmetric encryption
    b) Asymmetric encryption
    c) Hashing
    d) Tokenization

43. Which type of encryption uses a public and private key pair?
    a) Symmetric encryption
    b) Asymmetric encryption
    c) Hashing
    d) Steganography

44. Which is NOT an effective method of physical threat mitigation?
    a) Biometric authentication
    b) Surveillance cameras
    c) Unlocked server rooms
    d) Security guards

45. Patch management is important because:
    a) It keeps systems updated to fix vulnerabilities
    b) It removes old software
    c) It encrypts data automatically
    d) It trains employees

46. Which is a common way to mitigate phishing attacks?
    a) Disabling all email
    b) Employee training and email filtering
    c) Avoiding antivirus updates
    d) Using only public Wi-Fi

47. Which protocol secures email communication?
    a) SMTP over TLS
    b) FTP
    c) HTTP
    d) SNMP

Disclaimer: These are sample test questions of what a competitor will find in this competition. To view the official study guide, with the knowledge area and objective list, visit the guidelines on the Competitive Events page of the national website at www.fbla.org.

48. Which security measure helps protect against brute force attacks?
    a) Account lockout after repeated failed attempts
    b) Using short passwords
    c) Disabling antivirus software
    d) Enabling default admin accounts

49. Which is the primary purpose of intrusion detection systems (IDS)?
    a) Block all internet access
    b) Monitor network activity for suspicious behavior
    c) Replace firewalls
    d) Encrypt data

50. Which is an example of two-factor authentication?
    a) Password and security question
    b) Password and fingerprint scan
    c) Username and password
    d) PIN only

Disclaimer: These are sample test questions of what a competitor will find in this competition. To view the official study guide, with the knowledge area and objective list, visit the guidelines on the Competitive Events page of the national website at www.fbla.org.

Answer Key

1. B
2. C
3. B
4. C
5. B
6. D
7. C
8. B
9. C
10. B
11. B
12. C
13. A
14. B
15. C
16. A
17. B
18. B
19. B
20. A
21. A
22. B
23. B
24. B
25. B
26. B
27. A
28. A
29. C
30. B
31. C
32. B
33. B
34. A
35. B
36. B
37. B
38. A
39. A
40. B
41. B
42. A
43. B
44. C
45. A
46. B
47. A
48. A
49. B
50. B

Disclaimer: These are sample test questions of what a competitor will find in this competition. To view the official study guide, with the knowledge area and objective list, visit the guidelines on the Competitive Events page of the national website at www.fbla.org.