FUTURE BUSINESS LEADERS OF AMERICA (FBLA) CYBERSECURITY PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://fbla-cybersecurity.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

SAMPLE

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

SAMPLE

Questions

SAMPLE

1. What is the main function of L2TP?

A. To encrypt data for secure transactions

B. To support virtual private networks (VPNs)

C. To enhance wireless security

D. To provide direct internet access

2. What is ransomware?

A. A tool for encrypting files for protection

B. A type of malware that blocks access to data until a ransom is paid

C. A security feature used to protect online transactions

D. A program that cleans viruses from a computer

3. Which encryption method utilizes a combination of three keys, each 56 bits in length?

A. AES

B. Triple DES

C. RSA

D. Blowfish

4. In an incident response plan, what is the main focus during the recovery phase?

A. Identifying the security breach

B. Returning affected systems back to operations

C. Documenting the incident

D. Preventing future breaches

5. What is the importance of user training in cybersecurity?

A. To establish security protocols for IT departments

B. To educate employees about security risks

C. To encourage software updates and maintenance

D. To implement hardware solutions for security

SAMPLE

6. Which of the following describes malware that is specifically intended to harm businesses and individuals?

A. Adware

B. Malware

C. Spyware

D. Ransomware

7. Which technology is used to ensure the confidentiality of data during transmission over networks?

A. WPA

B. SSL

C. WEP

D. All of the above

8. What does 'defense in depth' refer to in cybersecurity?

A. A single security layer that protects against all threats

B. A strategy employing multiple layers of protection

C. A method for storing sensitive data

D. A framework for legal compliance

9. What does ciphertext refer to?

A. The original form of data

B. The readable format of encrypted data

C. The unintelligible form of data after encryption

D. A method of data compression

10. What is the focus of Executive Order 13636?

A. Improving personal privacy online

B. Increasing core capabilities to manage cyber risk in critical infrastructure

C. Regulating mobile phone data collection

D. Encouraging cybersecurity certifications

SAMPLE

Answers

SAMPLE

1. B
2. B
3. B
4. B
5. B
6. B
7. D
8. B
9. C
10. B

SAMPLE

Explanations

SAMPLE

1. What is the main function of L2TP?

A. To encrypt data for secure transactions

B. To support virtual private networks (VPNs)

C. To enhance wireless security

D. To provide direct internet access

The main function of Layer 2 Tunneling Protocol (L2TP) is to support virtual private networks (VPNs). It is a tunneling protocol that allows for the encapsulation of data packets, which enables secure communication over the internet. By creating a tunnel through which data is sent, L2TP helps connect remote users or branch offices to a central network, making it possible to securely transmit information across insecure networks like the internet. L2TP itself does not provide encryption or confidentiality; instead, it is often combined with other protocols such as IPsec (Internet Protocol Security) which handle the encryption aspect, enhancing the security of the VPN. This integration allows users to establish a secure connection while benefiting from the functionality and features provided by L2TP. Other options, while related to security or network connectivity in some way, do not accurately represent the primary role of L2TP in the context of VPNs, highlighting the specific purpose of L2TP in ensuring that data can be transmitted securely in a tunnel format between different points on a network, thus allowing seamless secure communications and connectivity.

2. What is ransomware?

A. A tool for encrypting files for protection

B. A type of malware that blocks access to data until a ransom is paid

C. A security feature used to protect online transactions

D. A program that cleans viruses from a computer

Ransomware is a form of malicious software designed to block access to data or systems until a ransom is paid to the attacker. When a device is infected with ransomware, the malware typically encrypts files, rendering them inaccessible to the user. The attacker then demands payment, usually in cryptocurrency, in exchange for the decryption key necessary to restore access to the affected files. This type of malware poses a significant threat as it can affect individuals, businesses, and organizations by locking them out of critical data and systems, leading to operational disruptions and potential financial losses. The method of operation relies on the urgency and desperation often felt by victims, compelling them to pay the ransom in hopes of retrieving their data. Other choices do not accurately describe ransomware. For instance, while encrypting files can be a part of ransomware's functionality, it is not a protective tool but rather an attack method. Security features for protecting online transactions focus on securing communication and data integrity, rather than extortion through data blockage. Moreover, a program designed to clean viruses serves a different purpose entirely, focusing on identifying and removing harmful software rather than manipulating data access for ransom.

SAMPLE

3. Which encryption method utilizes a combination of three keys, each 56 bits in length?

A. AES

B. Triple DES

C. RSA

D. Blowfish

The encryption method that utilizes a combination of three keys, each 56 bits in length, is Triple DES. This technique enhances the security provided by the original Data Encryption Standard (DES), which uses a single key for encryption. By applying DES three times with three different keys, Triple DES effectively increases the encryption strength. Triple DES operates on blocks of data and improves upon the vulnerabilities of single DES by utilizing the three keys in a specific sequence: the first key encrypts the data, the second key decrypts it, and the third key encrypts it again. This method significantly boosts security, making it much harder to break through brute force attacks, as the effective key length is significantly greater than that of DES alone. Other encryption methods mentioned do not utilize this particular key structure. AES, for example, employs key lengths of 128, 192, or 256 bits, and RSA is based on asymmetric key encryption rather than multiple symmetric keys. Blowfish uses a variable-length key but does not employ the triple key strategy that defines Triple DES. Thus, the distinctive feature of Triple DES being based on three 56-bit keys makes it the correct answer in this context.

4. In an incident response plan, what is the main focus during the recovery phase?

A. Identifying the security breach

B. Returning affected systems back to operations

C. Documenting the incident

D. Preventing future breaches

The main focus during the recovery phase of an incident response plan is to return affected systems back to operational status. This phase involves restoring systems, applications, and data that were impacted during the incident, ensuring that they are functioning correctly and securely before bringing them back online. The objective is to minimize downtime and restore business operations as quickly and efficiently as possible. This process may include activities like data restoration from backups, applying security patches, and verifying that any vulnerabilities have been addressed. It is crucial that systems are thoroughly checked for malware or any remaining security threats before fully resuming normal operations, to prevent further incidents. Other options such as identifying the security breach and documenting the incident are essential parts of the overall incident response process but belong to earlier phases. Preventing future breaches is also part of the longer-term planning that occurs after recovery, focusing more on updates and improvements to policies and controls rather than the immediate task of returning to normal operations.

SAMPLE

5. What is the importance of user training in cybersecurity?

A. To establish security protocols for IT departments

B. To educate employees about security risks

C. To encourage software updates and maintenance

D. To implement hardware solutions for security

User training in cybersecurity is crucial because it directly impacts how employees understand and respond to potential security threats. Educating employees about security risks helps them recognize phishing attempts, social engineering tactics, and other malicious activities that they may encounter in their daily work. When employees are well-informed about the types of threats that exist and the best practices to follow, they become an integral part of the organization's security posture. A significant portion of cybersecurity breaches is attributed to human error, such as clicking on malicious links or using weak passwords. Therefore, training programs that focus on raising awareness about these issues can substantially reduce the risk of such errors occurring. Furthermore, educated employees are more likely to adhere to security policies, report suspicious activities promptly, and make informed decisions when handling sensitive information. The other choices, while relevant to organizational security measures, do not focus directly on the role of employees in preventing cybersecurity threats. Establishing security protocols, encouraging software updates, and implementing hardware solutions are all important aspects of an organization's security strategy, but without a knowledgeable and vigilant workforce, these measures can fall short. User training fills that gap by empowering employees to recognize and respond effectively to security challenges.

6. Which of the following describes malware that is specifically intended to harm businesses and individuals?

A. Adware

B. Malware

C. Spyware

D. Ransomware

The term "malware" is a broad classification that encompasses any software designed to harm or exploit computers and networks. This category includes various types of malicious software, such as adware, spyware, and ransomware. The reason this answer is correct lies in the definition of malware itself, which inherently suggests malicious intent aimed at compromising systems, stealing information, or causing disruptions. While adware is specifically designed to generate revenue through advertisements and may not directly harm users, and spyware secretly monitors user activity without permission, ransomware is a subset of malware that specifically encrypts files and demands a ransom for decryption. By selecting "malware," you're capturing the overarching term that refers to harmful software aimed at both businesses and individuals, which aligns with the question's focus on software intended for harm. This classification allows for understanding the various threats each subtype represents, emphasizing the significance of recognizing and mitigating such risks in cybersecurity contexts.

SAMPLE

7. Which technology is used to ensure the confidentiality of data during transmission over networks?

A. WPA

B. SSL

C. WEP

D. All of the above

The correct answer highlights that SSL (Secure Sockets Layer) is a technology specifically designed to ensure the confidentiality of data during transmission over networks. It does this by encrypting the data being sent between a client and a server, which prevents unauthorized parties from intercepting and reading the information during transmission. WPA (Wi-Fi Protected Access) and WEP (Wired Equivalent Privacy) are both security protocols used to secure wireless networks. While they offer a level of protection against unauthorized access to the network, they are primarily focused on securing the connection itself rather than ensuring the confidentiality of the data being transmitted. WEP, for example, is considered outdated and vulnerable to various attacks, while WPA offers stronger security mechanisms than WEP but can still be susceptible in certain configurations. Therefore, while all these technologies contribute to network security, SSL is the key technology that specifically addresses the confidentiality of data in transit, making it the most suitable answer in this context.

8. What does 'defense in depth' refer to in cybersecurity?

A. A single security layer that protects against all threats

B. A strategy employing multiple layers of protection

C. A method for storing sensitive data

D. A framework for legal compliance

'Defense in depth' refers to a strategy that employs multiple layers of protection to safeguard an organization's data and systems. The idea behind this approach is that if one security layer fails, additional layers will still be in place to provide protection. This concept is crucial in cybersecurity because it recognizes that no single security measure can be entirely effective against all threats. Implementing multiple defenses allows organizations to create a more robust security posture. For example, a comprehensive security strategy might include firewalls, intrusion detection systems, encryption, access controls, and user training, among others. Each layer addresses different vulnerabilities and provides diverse mechanisms to counteract various types of attacks. This layered approach not only helps in mitigating risks but also serves to delay or complicate an attacker's progress, giving security teams more time to respond. By utilizing 'defense in depth,' organizations can better protect their valuable information and resources.

9. What does ciphertext refer to?

A. The original form of data

B. The readable format of encrypted data

C. The unintelligible form of data after encryption

D. A method of data compression

Ciphertext refers to the unintelligible form of data that results from the process of encryption. When plaintext, which is the readable form of data or information, undergoes encryption using specific algorithms and keys, it transforms into ciphertext. This transformation is designed to protect the confidentiality of the data, ensuring that it cannot be easily understood or accessed by unauthorized individuals. The effectiveness of encryption lies in the fact that without the appropriate decryption key or algorithm, turning ciphertext back into readable data (plaintext) is highly difficult or impossible, thus maintaining data security. The other choices do not align with the definition of ciphertext. The original form of data is known as plaintext, while the readable format of encrypted data refers to plaintext as well. Additionally, a method of data compression involves reducing the size of data, which is unrelated to the concept of encryption and ciphertext.

SAMPLE

10. What is the focus of Executive Order 13636?

A. Improving personal privacy online

B. Increasing core capabilities to manage cyber risk in critical infrastructure

C. Regulating mobile phone data collection

D. Encouraging cybersecurity certifications

Executive Order 13636, signed by President Obama in 2013, focuses specifically on enhancing the security and resilience of the nation's critical infrastructure against cyber threats. This initiative emphasizes the need for federal engagement and support in helping organizations improve their cybersecurity capabilities. By establishing a framework for managing cyber risks, the executive order directs various federal agencies to collaborate with private sector partners to enhance their core cybersecurity capabilities. The order recognizes that critical infrastructure sectors, such as energy, transportation, and communications, are essential for national security and economy, and thus it prioritizes the management of cyber risks in these fields. This overarching goal of improving the nation's cybersecurity posture, particularly in critical infrastructure, is a cornerstone of the executive order's intent. The other options focus on related but distinct areas such as personal privacy, mobile data regulation, and cybersecurity certifications, which are not the primary focus of this executive order.

SAMPLE

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://fbla-cybersecurity.examzify.com

We wish you the very best on your exam journey. You've got this!

SAMPLE