ISC^2

Certified in Cybersecurity

MCQ ISC2 CC Chapter 2:Incident Response, Business Continuity and Disaster Recovery Concepts

Based on documentation by WAN MUHAMMAD AZIM BIN WAN MOHD HAZAN AMRI

7/11/2022

Disclaimer

I used Claude.ai to make this MCQ practice exam by referencing Wan Azim's documentation of ISC2 CC. Claude.ai is used to extract information and create questions alongside their answers.

Huge thanks to Wan Azim for documenting the ISC2 Certified in Cybersecurity course!
For more write-ups or documentation check out my repo at:
https://github.com/MikhailAmzar/reports

Incident Response, Business Continuity and Disaster Recovery Concepts

Here is a 50-question exam covering the main topics from Chapter 2: Incident Response, Business Continuity and Disaster Recovery Concepts.

1. What is the primary goal of incident management?
A. To prevent all incidents
B. To be prepared
C. To assign blame
D. To increase security budget

2. Which of the following is defined as "any observable occurrence in a network or system"?
A. Incident
B. Event
C. Exploit
D. Intrusion

3. What is a breach?
A. Any cybersecurity incident
B. The unauthorized disclosure of personally identifiable information
C. A system vulnerability
D. A type of malware

4. What is the first priority in any incident response?
A. Protecting the organization's reputation
B. Preserving evidence
C. Protecting life, health, and safety
D. Restoring systems to normal operation

5. Which of the following is NOT a common component of an incident response plan?
A. Preparation
B. Detection and Analysis
C. Financial Assessment
D. Post-Incident Activity

6. What does CSIRT stand for?
A. Computer Security Incident Response Team
B. Cybersecurity Incident Reporting Team
C. Critical System Incident Recovery Team
D. Computer System Information Research Team

7. Who should be involved in creating a Business Continuity Plan (BCP)?
A. Only the IT department
B. Only senior management
C. Only the security team
D. Members from across the organization

8. What is the main difference between Business Continuity (BC) and Disaster Recovery (DR)?
A. BC is about maintaining critical business functions, while DR is about restoring IT and communications
B. BC is for small incidents, while DR is for large incidents
C. BC is a technical function, while DR is a business function
D. There is no significant difference

9. What is a zero-day vulnerability?
A. A vulnerability that has existed for zero days
B. A previously unknown system vulnerability
C. A vulnerability with zero impact
D. A vulnerability in day zero of software development

10. Which of the following is an example of an exploit?
A. A system crash
B. A particular attack that takes advantage of a vulnerability
C. An unknown vulnerability
D. A potential threat

11. What does BIA stand for in the context of business continuity?
A. Business Impact Analysis
B. Basic Incident Assessment
C. Breach Investigation Algorithm
D. Business Intelligence Application

12. What is the main goal of a Disaster Recovery Plan (DRP)?
A. To prevent disasters from occurring
B. To guide actions until the business is restored to full last-known reliable operations
C. To assign blame for the disaster
D. To document lessons learned after a disaster

13. Which of the following is NOT one of the four primary responsibilities of a CSIRT when an incident occurs?
A. Determine the amount and scope of damage
B. Implement necessary recovery procedures
C. Fire the employees responsible for the incident
D. Supervise implementation of additional security measures

14. What does "BC" stand for in information security?
A. Before Crisis
B. Business Continuity

C. Breach Containment
D. Baseline Configuration

15. In the context of incident response, what does the term "containment" refer to?
A. Preventing the incident from spreading or causing further damage
B. Putting all the incident evidence in a secure container
C. Restraining the personnel involved in the incident
D. Classifying the incident information

16. What is an intrusion?
A. Any observable occurrence in a system
B. A security event where an intruder gains or attempts to gain unauthorized access
C. Any circumstance with the potential to impact operations
D. A weakness in an information system

17. Which of the following is a key part of a business continuity plan?
A. Communication
B. Blame assignment
C. System redesign
D. Employee termination

18. What does the "Preparation" phase of an incident response plan involve?
A. Developing a policy and training staff
B. Analysing the incident
C. Choosing a containment strategy
D. Documenting lessons learned

19. Who are typically the first responders for IT incidents?
A. Law enforcement
B. Senior management
C. IT professionals
D. Human resources

20. What is a vulnerability in the context of information security?
A. A type of malware
B. A weakness that could be exploited by a threat source
C. An exploit
D. A security policy

21. What should be done in the "Post-Incident Activity" phase of incident response?
A. Monitor all possible attack vectors
B. Choose a containment strategy
C. Document lessons learned
D. Implement an incident response team

22. Which of the following is NOT typically a member of an incident response team?
A. Information security professionals
B. Customer service representatives

C. Legal representatives
D. Engineering representatives

23. What is the difference between an event and an incident?
A. There is no difference
B. An event is harmless, while an incident has the potential to disrupt the business's mission
C. An incident is harmless, while an event has the potential to disrupt the business's mission
D. Events only occur in IT systems, while incidents can occur anywhere

24. What does DR stand for in the context of this chapter?
A. Data Retention
B. Disaster Recovery
C. Damage Report
D. Digital Rights

25. In a disaster recovery scenario, why is it important to have multiple levels of backup?
A. To confuse potential attackers
B. To provide options for partial recovery
C. To address different retention period needs and avoid reinfection
D. It's not important, one backup is sufficient

26. What type of plan document provides a high-level overview of the disaster recovery plan?
A. Technical guide
B. Department-specific plan
C. Executive summary
D. Checklist

27. What is the primary focus of Business Continuity Planning (BCP)?
A. Restoring IT systems
B. Sustaining business operations
C. Improving cybersecurity
D. Training employees

28. Which of the following is NOT a common component of a comprehensive business continuity plan?
A. List of BCP team members
B. Detailed technical specifications of all IT systems
C. Notification systems and call trees
D. Immediate response procedures and checklists

29. What is the main difference between incident response and disaster recovery?
A. Incident response is reactive, while disaster recovery is proactive
B. Incident response focuses on security incidents, while disaster recovery focuses on restoring IT services after any disruption
C. Incident response is for small-scale events, while disaster recovery is for large-scale events
D. There is no significant difference

30. What does the term "adverse event" refer to?

A. Any observable occurrence in a network
B. An event with negative consequences
C. A deliberate attack on a system
D. A natural disaster affecting IT infrastructure

31. Who should have access to the full copies of the Disaster Recovery Plan?
A. All employees
B. Only the CEO
C. Critical disaster recovery team members
D. The general public

32. What is the purpose of a Business Impact Analysis (BIA)?
A. To identify and prioritize system recovery requirements
B. To determine the financial cost of a security breach
C. To assess employee performance during a crisis
D. To test the effectiveness of security controls

33. Which of the following is a key characteristic of a zero-day vulnerability?
A. It has existed for a long time
B. It is well-known to security professionals
C. It cannot be exploited
D. It does not fit recognized patterns or signatures

34. What does SOC stand for in the context of information security?
A. System Operations Center
B. Security Oversight Committee
C. Security Operations Centre
D. Secure Online Communications

35. What is the main goal of the "Detection and Analysis" phase in incident response?
A. To prevent incidents from occurring
B. To identify and understand the scope of an incident
C. To restore normal operations
D. To improve future security measures

36. Which of the following is NOT a typical responsibility of a Security Operations Centre?
A. Monitoring events on the network
B. Developing new software applications
C. Detecting security incidents
D. Analyzing security events

37. In the context of incident response, what does "exploitation" refer to?
A. Taking advantage of employees
B. A specific attack that leverages a system vulnerability
C. Exploring new technologies
D. Expanding business operations

38. What should be included in the "Containment" phase of incident response?

A. Training staff on incident response
B. Implementing an incident response team
C. Gathering evidence and isolating the attack
D. Documenting lessons learned

39. Which statement best describes the relationship between Business Continuity and Disaster Recovery?
A. They are completely unrelated concepts
B. Disaster recovery is a subset of the larger discipline of business continuity
C. Business continuity is a subset of disaster recovery
D. They are different terms for the same concept

40. What is the primary purpose of having technical guides in a Disaster Recovery Plan?
A. To provide high-level overviews for executives
B. To help IT personnel implement and maintain critical backup systems
C. To serve as checklists for managers
D. To communicate with the public during a crisis

41. What does the "IR" in "IR Plan" stand for?
A. Information Retention
B. Incident Response
C. IT Recovery
D. Internal Regulation

42. Which of the following is a characteristic of a good incident response plan?
A. It is kept confidential and known only to top management
B. It is rigid and doesn't allow for flexibility
C. It is shaped by the organization's vision, strategy, and mission
D. It focuses solely on technical aspects of incident response

43. What is the purpose of a phone tree in a Business Continuity Plan?
A. To provide entertainment during a crisis
B. To ensure that critical personnel can be contacted if one person is unavailable
C. To track employees' personal phone usage
D. To order food delivery during an incident

44. In the hospital example from the document, why couldn't they use their last backup to recover from the incident?
A. They didn't have any backups
B. The backups were corrupted by time-based malware
C. The backups were too old
D. They lost the encryption keys for the backups

45. What is the main function of a Computer Security Incident Response Team (CSIRT)?
A. To develop new security software
B. To investigate and respond to computer security incidents
C. To manage the organization's budget
D. To hire and fire IT personnel

46. What should managers and public relations personnel have during a disaster recovery situation?
A. Technical guides with detailed system information
B. The authority to fire employees involved in the incident
C. Simple-to-follow, high-level documents to help them communicate accurately
D. Access to all confidential data

47. Which of the following best describes the difference between an event and an exploit?
A. An event is malicious, while an exploit is benign
B. An event is any observable occurrence, while an exploit is a specific attack
C. An exploit is any observable occurrence, while an event is a specific attack
D. There is no difference between the two terms

48. What is the primary goal of business continuity planning?
A. To eliminate all risks
B. To sustain critical business operations during a disruption
C. To reduce IT costs
D. To improve customer satisfaction

49. In the context of incident response, what does "critical data" refer to?
A. All data stored on the organization's systems
B. Only financial data
C. Data essential for the organization's mission or business objectives
D. Personal data of the employees

50. What is an important consideration when developing recovery strategies for complex systems?
A. Focus only on individual servers
B. Ignore dependencies between systems
C. Understand the flow of data and intricate dependencies between systems
D. Recover all systems simultaneously

Answer Key: Chapter 2

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