



MCQ on Cyber Security

- Q.1 Which of these is not a member of Information Security Steering Committee (ISSC) ?
- A. GM (CTO)
 - B. GM (I&C)
 - C. GM (Legal)
 - D. GM(Accounts)

ANS: D

- Q.2 Which of these is not correct about CISO (Chief Information Security Officer)?
- A. CISO must be a senior level functionary in the bank
 - B. He should be appointed for a reasonable minimum term
 - C. He should report directly to the MD and CEO of the Bank
 - D. He should have the requisite technical background and expertise

ANS: C

- Q.3 Out of these four aspects ,which aspect is not addressed by Cyber Crisis Management Plan (CCMP)?
- A. Detection
 - B. Prevention
 - C. Recovery
 - D. Containment

ANS: B

- Q.4 What is Daksh Portal?
- A. A web based RBI portal for compliance monitoring
 - B. A web based RBI portal for monitoring of NBFCs
 - C. RBI portal for reorting Counterfeit currency notes
 - D. It is a new name given to CRILC portal

ANS: A

- Q.5 what is full form of NCIIPC?
- A. National Critical Information Infrastructure Protection Centre
 - B. National Critical Information Infrastructure Prevention Centre
 - C. National Clearing Information Infrastructure Prevention Centre
 - D. National Clearing Information Infrastructure Protection Centre

ANS: A



MCQ on Cyber Security

- Q.7 Which of the fact is /are true with reference to the Cyber Security Policy? The Policy document is organized under the following volumes 1.Cyber security policy Framework 2.Cyber Security Set-up 3. Cyber security policy Exception 4.Cyber security policy Violation
- A. only 1 and 2
 B. 1,2 and 3
 C. 2 and 3 only
 D. all 1,2,3 and 4

ANS: D

- Q.8 Which of these statement is/are correct about System Owners?
- A. The System Owners are responsible for the actual computers that house the data
 B. System Owner is typically an official at Top Management level who heads people and process at each business unit
 C. General Manager/Deputy General Manager/Department Head of IT Department shall be designated as System Owner for systems held at DC, DR and Near DR
 D. all are correct

ANS: D

- Q.9 What is full form of IDRBT?
- A. Institute for Development and Research in Banking Technology
 B. Institute for Design and Research in Banking Technology
 C. Indian Development Research Institute for Banking Technology
 D. None of the above

ANS: A

- Q.10 Minimum _____level officers from ISSD., Information Technology Dept. and Digital Banking Division to be nominated to champion the implementation and monitoring of Cyber Security
- A. Sr Manager/Manager
 B. CM/AGM
 C. AGM/DGM
 D. DGM/GM

ANS: B

- Q.11 Who has the the overall responsibility for monitoring the implementation of Security Polices and Standards ?
- A. The deptment Head,ITD
 B. CISO



MCQ on Cyber Security

- C. The department Head,DBD
- D. ED looking after ITD

ANS: A

Q.13 What is Man-in-the-middle (MitM) attack?

- A. a network security attack where an individual tries to steal the information that smartphones, computers and other digital devices send or receive
- B. when a hacker inserts itself between the communications of a client and a server.
- C. the millions of systems infected with malware under hacker control in order to carry out Distributed Denial-of-Service attacks
- D. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application

ANS: B

Q.14 Social Engineering involves

- A. a tool for detecting Cyber security fraud
- B. Motivate peoples to make IT engineering to avoid cyber fraud
- C. Organize Online webinars to regarding Cyber security frauds
- D. psychologically manipulating people into divulging information or taking inappropriate actions

ANS: D

Q.15 Business email compromise (BEC) also known as

- A. Eavesdropping Attack
- B. Drive-by attack
- C. CEO fraud or Whale Phishing
- D. Distributed Denial-of-Service (DDOS)

ANS: C

Q.16 What is SQL Injection Attack ?

- A. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application
- B. It involves injecting malicious code into a website, and thereby Stealing or dumping customer information from the website
- C. It is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated
- D. It involves targeting a system with flood of incoming messages, connection requests or malformed packets by a



MCQ on Cyber Security

number of compromised systems to slow down or crash it.

ANS: B

Q.17 What is RANSOM WARE ? Choose the best option.

- | | |
|--|--|
| A. Cyber criminals ask for ransom money in lieu of unblocking the network which they had blocked | B. Ransom ware is a type of malware that blocks access to a victim's files through encryption and demands money to restore that access |
| C. Cyber Criminals threaten the system administrator for hacking the system and ask for meney for not doing it | D. None of these |

ANS: B

Q.19 What is CERT-In?

- | | |
|--|--|
| A. The Indian Computer Emergency Response Team (CERT-In) is an office within the Ministry of Science and Technology . | B. The Indian Computer Emergency Response Team (CERT-In) is an office within the Ministry of Electronics and Information Technology. |
| C. The Indian Computer Emergency Response Team (CERT-In) is an office within the Ministry of Information and Broadcasting. | D. The Indian Computer Emergency Response Team (CERT-In) is an office within the Ministry of AYUSH. |

ANS: B

Q.20 What is true about Cyber Security Policy of the bank?

- | | |
|--|---|
| A. Cyber Security Policy is to be distinct from the broader IT Policy / IS Security Policy of a bank | B. Cyber security policy is a part of broader IT security policy of the Bank. |
| C. There is no need of Cyber Security policy seperately. | D. None of the above |

ANS: A
