MBSC-4.2 G

Sl.No. :

Total No. of Pages : 2

Fourth Semester M.B.A. Degree Examination, November - 2024
(SLM Scheme) (CBCS)
MANAGEMENT
Information Technology (ElectiveG)
Information Security

Time : 3 Hours **Max. Marks : 80**

SECTION - A

Answer any five sub-questions. Each question carries 5 marks. [5 × 5 = 25]

Q1) Why is it important to have a strong password policy, and what are some key elements of an effective password discipline?

Q2) Explain the difference between threats and vulnerabilities in the context of cyber security.

Q3) What are some common security weaknesses in operating systems?

Q4) What are the primary functions of switches, routers and firewalls in a network?

Q5) What are the key objectives of the Information Technology Act 2000 and how does it address cybercrime in India?

Q6) State the importance of conducting regular cyber security audits.

Q7) Identify the most common identity management protocols used in modern web applications?

SECTION - B

Answer any four questions. Each question carries 10 marks. [4 × 10 = 40]

Q8) What is the role of Active Directory and Kerberos in a Windows environment and how do they help in securing user authentication and access control?

Q9) Examine the common risks associated with email and how can these risks be mitigated?

Q10) What role do security information and event management play in enhancing the effectiveness of these systems?

Q11) Explain the advantages and disadvantages of using symmetric key algorithms for securing communication between parties?

Q12) What are Cyber security audits? What critical areas should be assessed during these audits to ensure comprehensive security?

Q13) Provide the core components of cyber security and how do they work together to protect information and systems from cyber threats?

SECTION - C

Q14) **Case (Compulsory) :** **[1 × 15 = 15]**

A mid-sized financial institution, GlobalBank, has recently experienced a significant data breach that exposed sensitive customer information, including personal identification details, account numbers, and transaction histories. The breach occurred due to a combination of factors, including outdated software, insufficient employee training and inadequate security protocols.

GlobalBank's management had previously recognized the growing threat of cyber attacks but had not yet developed a comprehensive cyber security policy. The breach has not only led to financial losses and reputational damage but has also attracted regulatory scrutiny.

In the aftermath, GlobalBank's executives are now urgently working to develop a comprehensive cyber security policy to prevent future incidents. They are considering various aspects such as data protection, employee training, incident response and collaboration with law enforcement agencies.

Questions :

a) What key elements should GlobalBank include in its comprehensive cyber security policy to address the vulnerabilities that led to the data breach and how can these measures help in preventing future incidents?

b) How can GlobalBank ensure that its cyber security policy remains effective over time, considering the evolving nature of cyber threats and regulatory requirements?

▽▽▽▽