NEW SYLLABUS

544

Roll No. .....

OPEN BOOK EXAMINATION

Time allowed : 3 hours

Maximum marks : 100

Total number of questions : 4

Total number of printed pages : 12

NOTE : *Answer **ALL** Questions.*

1. TechCorp is a leading player in the IT industry, providing a range of software solutions and digital services to clients worldwide, recognized the need to bolster its cybersecurity defences and comply with the provisions of the IT Act 2000. Facing challenges posed by manual audit procedures and the dynamic nature of cyber threats, TechCorp partnered with a prominent AI solutions provider specializing in cybersecurity. Together, they deployed an AI-driven security audit platform tailored to the organization's infrastructure and regulatory requirements. The platform utilized machine learning algorithms to analyse network traffic, identify anomalous behavior, and detect potential security breaches in real-time. Additionally, NLP capabilities enabled the platform to interpret regulatory texts, extract relevant compliance mandates from the IT Act 2000, and align audit findings with legal requirements.

TechCorp encounters several challenges in ensuring compliance with relevant cybersecurity regulations. The cybersecurity legal framework is intricate, with multiple regulations and standards to adhere to, including industry-specific guidelines and international norms. The company must adapt its cybersecurity practices to mitigate emerging cyber threats, such as ransomware attacks, data breaches, and insider threats. Allocating sufficient resources, including budget, personnel, and technology, poses a challenge for TechCorp to implement robust cyber security measures effectively.

To address these challenges and enhance cyber security compliance, TechCorp conducting a risk assessment thorough assessment of cyber security risks and vulnerabilities across the organization's digital infrastructure, including networks, systems, and applications. Engaging legal experts to conduct a comprehensive review of cyber security-related laws, regulations, and industry standards applicable to TechCorp's operations, identifying gaps and areas for improvement.

TechCorp uses AI-powered audit platform, which can detect the threat automatically by continuously monitored network activities and system logs to identify suspicious patterns indicative of cyber threats, such as malware infections, unauthorized access attempts, and data exfiltration. Through semantic analysis and regulatory mapping algorithms, the platform correlated audit findings with specific provisions of the IT Act 2000, facilitating regulatory compliance assessments and audit reporting.

Deploying robust security controls and technologies, such as multi-factor authentication, and intrusion detection systems, to fortify the company's cyber defences and mitigate potential threats 'TechCorp organizing cyber security training sessions and awareness campaigns to educate employees about best practices, security protocols, and their roles in safeguarding sensitive information.

By proactively addressing cyber security challenges and enhancing compliance efforts. TechCorp achieves the strengthened cyber security posture enables the company to better withstand cyber threats and minimize the impact of potential security incidents. Demonstrating a commitment to cyber security compliance fosters trust among customers, partners, and stakeholders, enhancing the company's reputation and competitive advantage in the market.

In an increasingly digitized and interconnected business environment, cyber security compliance is imperative for organizations to safeguard their assets, protect customer data, and mitigate risks effectively. By embracing a proactive approach to cyber security assessment and compliance, TechCorp demonstrates its commitment to maintaining the highest standards of security and resilience in the face of evolving cyber threats and regulatory requirements.

In the above case scenario, answer the following questions :

(*a*) The use of Artificial Intelligence is increasing in the field of cyber security day by day. Give any five benefits of Artificial Intelligence in cyber security.

(*b*) For TechCorp, what are security errors that users generally commit and steal sensitive information ? Also advice the solution to these challenges.

(*c*) TechCorp organizes a training on IT Act, 2000 to sensitize their employees for disclosure of information and for data protection and privacy. State the related sections corresponding to these penalties.

(*d*) State any five points that need to be followed to prevent data loss prior to disclosure to forensic experts.

(*e*) Security audits are often used to determine compliance with regulations such as Information Technology Act, 2000. Elucidate the statement with reference to significance of Security Audit.

(*5 marks each*)

2. Mr. A is working as a CEO in a leading financial institution. On weekends, he spends time with family and on his hobbies like photography, singing and reading books. He is also active on various social media platforms and uploads their activities on the platforms. Last month, he participated in a professional photography exhibition and presented his

photographs to viewers and got appreciation and won award for that. After some time, he found some threat posts on his social media platforms and he becomes a victim of online harassment and cyberbullying. The perpetrator continuously posts defamatory content and threats against Mr. A, causing significant distress and reputational damage.

IT Analyst of Mr. A's Company discovers a data breach compromising sensitive customer information, including banking credentials and personal details. 'The breach exposes thousands of customers to identity theft and financial fraud raising concerns about data protection and cyber security. The aim of the Mr. A's organization is to prevent any data breach incident before any malware is able to access network server or before vulnerabilities in the software are exploited by hackers.

One day Mr. A found that his copyrighted images being used without authorization on various websites and social media platforms. Despite his efforts to request the removal of infringing content, the unauthorized use persists, leading to financial losses and infringement of his intellectual property rights.

His wife is an active social worker and she post the social work activities governed by her on the social media like Facebook and Instagram. She is a shopping lover and lost her credit card last week in the market and forgot to take action on missing credit cards. Recently she received a series of obscene messages from an unknown number. The accused also sent emails to her and created a fake account on Facebook containing morphed and offensive images of her. She receives a message from the bank about the deduction of some amount against online purchasing. An online marketplace experiences a surge in fraudulent transactions, with perpetrators using her stolen credit card information to make unauthorized

purchases. The fraudulent activities result in financial losses for both the e-commerce platform and affected her with mental stress. She suggests to the e-commerce platform for the need of apply robust cyber security measures and fraud detection mechanisms.

Legal experts analyze each scenario of Mr. A's Family in light of relevant Indian cyber laws, judicial precedents, and established legal principles to determine the appropriate legal recourse and potential liabilities for the parties involved. Based on the specific facts and circumstances of each case, strategies are developed to address the legal challenges, protect the rights of victims, and ensure compliance with regulatory requirements. Through litigation, negotiation, or alternative dispute resolution mechanisms, legal professionals work towards achieving favorable outcomes for their clients, whether it involves obtaining compensation for damages, securing injunctions, or prosecuting cybercrime offenders.

In the above case scenario, answer the following questions :

(*a*) What are the various legal provisions of IPC under which the court can take judgement against accused who sent emails to Mr. A's wife and created her fake account on Facebook that contain the morphed and offensive images ?

(*5 marks*)

(*b*) On a complaint filed by Mr. A for the alleged identity theft committed by a cyber criminal named X, a police inspector was appointed to investigate cyber offence. The police inspector sent the laptop to Mr. A to the forensic lab for further analysis and investigation. The forensic lab used sophisticated methods to analyse the information contained in these hard drives, email accounts, social networking sites, and other digital archives to retrieve and assess any information that can serve as a viable evidence

to prove that X committed cyber crime. Which field of technology will be used as investigative techniques to identify and store evidence from a computer ? Also state its types.

(*5 marks*)

(*c*) Mr. A's wife lost her cards in the shopping mall. After this incident, she wants to switch to online e-commerce that enables users to access online shopping platforms without the use of a desktop computer, through wireless handheld devices. What are the three basic functions can be used to categorize M-commerce ?

(*5 marks*)

(*d*) Software security is a type of proactive security and it is based on the principle "prevention is better than cure". Proactive security typically necessitates additional software and hardware designed for spotting threats before they turn into serious incidents. In this context, what can be the various benefits of proactive security for an organization ?

(*5 marks*)

(*e*) Mr. A’s wife decides to use the digital currency for the payment in the purpose to prevent any type of fraud in the payment. Advise her various pros and cons of using the digital currency.

(*5 marks*)

3. In today's digital era, online banking has become an integral part of the banking sector, offering convivence and accessibility to customers worldwide. However, with the increasing reliance on Internet based services, ensuring the security of online banking platforms has become

a paramount concern for banks and financial institutions. The online banking platform utilizes internet and related technologies to facilitate seamless transactions and user transactions. This includes the use of secure protocols to encrypt data transmission between user and banking servers. This infrastructure and protocols are employed to guarantee high availability and reliability of banking services, minimize downtime and service disruptions.

Software security is also a critical aspect of the online banking platform, encompassing various measures to protect against security threats and vulnerabilities. Secure coding practices are followed during the development phase to minimize the risk of common security flaws such as SQL injection, cross-site scripting (XSS), and buffer overflows. Regular code reviews, vulnerability assessments, and penetration testing are conducted to identify and address security issues proactively. Additionally, the platform incorporates mechanisms for user authentication, session management, and access control to prevent unauthorized access to sensitive resources and functionalities. To increase the security in customer's data some platform can use that asymmetric encryption algorithms such as RSA to establish secure communication channels. Digital certificate issued by Certifying Authorities (CA) are used to verify the authenticity of the banking servers and protect against the man in middle attack.

The IT Security team of XYZ Bank discovers suspicious activity on its computer network, indicating a potential data breach. Bank's IT security team initiates a forensic investigation to identify the source of the breach, recover lost data, and ensure compliance with relevant regulations and ethical standards. The key issues are related with Data Recovery Procedures and data protection in which implementing ethical data recovery procedures to retrieve lost or compromised data, while preserving the integrity of digital evidence. Ensuring proper

precautions are taken during the gathering of digital evidence to maintain its admissibility in legal proceedings and prevent contamination or tampering. Now Bank Employing computer forensics software tools and forensic toolkits to recover deleted or hidden files, analyze system artifacts and cross-validate findings in computer evidence-related cases.

In this regard, the forensic team at XYZ Bank follows established protocols for data recovery and evidence handling, ensuring compliance with legal and ethical standards throughout the investigation. By conducting a thorough time-line analysis of computer files. the team enabling prompt remediation and risk mitigation measures. Advanced forensic tools and software are utilized to recover deleted files, analyze system artifacts, and corroborate findings, strengthening the integrity of digital evidence presented in legal proceedings. The investigation also highlights the importance of data protection and privacy regulations in safeguarding sensitive information and maintaining customer trust and compliance with regulatory requirements.

In the above case scenario, answer the following questions :

(*a*) What guidelines does XYZ Bank's IT security team follow to initiate a computer forensic analysis upon discovering suspicious activity on its computer network ?

(*5 marks*)

(*b*) When dealing with a massive amount of data, often companies suffer data loss which needs to get recovered. It is important to choose a backup solution that addresses a wide range of restore and recovery needs and reduces data recovery steps. As a member of IT security team, explain the various types of data recovery that may be needed for any financial organization ?

(*5 marks*)

(*c*) Secure Protocols usually make use of cryptography and encryption techniques to secure and encrypt data, which can only be decrypted by using special algorithm, logical key, formula or a combination of them. What are the various commonly used secure protocols that can be used in data transmission of XYZ Bank services ?

(*5 marks*)

(*d*) Certification Authorities (CA) such as VeriSign are organizations that issue digital certificates to applicants whose identity, they are willing to vouch for. Each certificate is linked to the certificate of the CA that signed it. As an IT expert explain the various responsibilities of Certification Authorities.

(*5 marks*)

(*e*) Software Security refers to the practice of developing and engineering the software in a manner which keeps it secure from external malicious attacks, while also ensuring that in case of any such attack, the software does not malfunction and continues to operate. As an IT engineer in Bank, explain any 5 software security goals to be achieved.

(*5 marks*)

4. ABC Corporation, a multinational company known for its innovative products and services, is using the advanced data analytics tools for massive amount of data on current market trends and understand the customer preferences, and using MIS to track sales, inventory and related business information for streamline its operations. The company recently implemented an ERP system for enhanced collaboration between customers and vendors, inventory management, pricing strategies, marketing campaigns and support services. The company migrated its operational data on the cloud for enhanced accessibility and scalability. The company facing

the challenges in the efficiently managing its operations, while ensuring seamless customer experiences. However, unforeseen challenges have arisen, prompting the need for a comprehensive approach to data management and recovery.

The Company employs a decision support system tool to analyse sales data, market trend and customer behaviour, purchasing pattern and also helps in making informed decision. By analyzing the purchase patterns, it can predict demand for specific products and adjust inventory levels accordingly, reducing stockouts and optimizing resources. ABC automates routine administrative tasks such as email communication, document management, and scheduling. This streamlines internal processes, improves collaboration among employees, and enhances overall operational efficiency like automated email responses and document templates save time for customer service representatives, enabling them to focus on addressing customer inquiries promptly. During routine operations, ABC Corporation face difficulties in recovering internet usage data from network logs, browsing histories and cloud services to trace the activities of the attackers and understand the breach methods. The lack of comprehensive internet data recovery tools hindered the company ability to uncover critical information about the cyber-attack. In the solution of this problem the company invested in robust internet data recovery tools to retrieve and analyse the Internet data usage for investigation purposes. The company leveraged advanced forensic techniques to trace the attack activities online and gain insight in to the breach methods. ABC Corporation also engages forensic experts to gather evidence related to the data breach and identify potential vulnerabilities in its systems. It must follow stringent protocols for evidence collection, preservation, and chain of custody to ensure admissibility in legal proceedings. Meanwhile, the company takes proactive measures to strengthen cyber security defences, including regular vulnerability assessments, employee training on data security best practices, and implementation of encryption protocols.

As part of the investigation, ABC Corporation seeks to recover internet usage data to trace the source of the data breach. It collaborates with internet service providers and utilizes specialized tools to retrieve relevant information while adhering to legal and ethical guidelines governing data collection and privacy rights. The company recognizes the importance of transparency and consent in accessing user data and ensures compliance with applicable regulations.

ABC Corporation evaluates the effectiveness of its MIS, ERP, and cloud computing systems in facilitating data management and decision-making processes. It identifies areas for improvement, such as enhancing data governance practices, integrating advanced analytics capabilities, and implementing robust disaster recovery plans. The company remains committed to leveraging technology responsibly and ethically to drive business growth while safeguarding data integrity and security.

In the above case scenario, answer the following questions :

(*a*) When dealing with a massive amount of data, often companies suffer data loss which needs to get recovered. For the purpose of data recovery, what are some common scenarios where data recovery procedures would be necessary ?

(*5 marks*)

(*b*) List out the benefits of migrating operational data to the cloud for create infrastructure as a service for ABC Corporation.

(*5 marks*)

(*c*) Decision Support Systems (DSS) are interactive software-based systems intended to help managers in decision-making by accessing large volumes of information generated from various related information. Mention any five key attributes of DSS that help the managers of ABC Corporation to take decision.

(*5 marks*)

(*d*) A management information system (MIS) is a computerized database of financial information organized and programmed in such a way that it produces regular reports on operations for every level of management in a company. Explain the importance of MIS in ABC Corporation in providing support services.

(*5 marks*)

(*e*) ABC Corporation uses data protection practices to demonstrate to their customers and users that they can be trusted with their personal data. State some of the challenges that ABC Corporation may face when protecting user privacy.

(*5 marks*)

———— o ————