

GUJARAT TECHNOLOGICAL UNIVERSITY
MBA-SEMESTER-III-EXAMINATION-WINTER-2024

Subject Code: 1539604**Date: 16/12/2024****Subject Name: Cyber Security and Information Technology Governance****Time: 10:30 AM TO 01:30 PM****Total Marks: 70****Instructions:**

1. Attempt all questions.
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.
4. Use of simple calculators and non-programmable scientific calculators are permitted.

Q. No.	Question Text and Description	Marks
Q.1	Definitions / terms / explanations / short questions based on concepts of theory/practical (a) Incident Response (b) Cyber Defamation (c) Spamming (d) Email spoofing (e) Phishing (f) Firewall (g) Zero Trust	14
Q.2	(a) Describe the security implications of mobile and wireless devices for organizations	07
	(b) What are botnets and attack vectors?	07
OR		
	(b) Discuss the challenges and risks associated with cybercrime in cloud computing	07
Q.3	(a) Discuss the concept of social engineering, explaining how criminals use psychological manipulation to commit cyber offenses and providing examples	07
	(b) What is identity theft?	07
OR		
Q.3	(a) Detail Question -Explain salami attack technique, data diddling and web jacking	07
	(b) What are the key benefits of implementing IT Governance	07
Q.4	(a) Discuss the significance of cyber laws in India	07
	(b) Why is incident handling an essential component of cybersecurity in organizations?	07
OR		
Q.4	(a) Discuss web threats organizations face & their implications for security and privacy	07
	(b) What is phishing, and what are the common methods used by attackers?	07

Q.5

CASE STUDY: Cyber Attack on TechCorp

Background:

TechCorp, a leading technology firm, suffered a devastating ransomware attack. Hackers gained access to the company's network through a vulnerable employee laptop. The malware spread rapidly, encrypting sensitive data and crippling TechCorp's operations.

Investigation:

1. The attackers demanded a hefty ransom in cryptocurrency to restore access to the encrypted data.
2. TechCorp's cybersecurity team discovered that the employee's laptop had not been updated with the latest security patches.
3. The company's backup systems were also found to be inadequate, making it difficult to recover lost data.

Response by TechCorp:

1. TechCorp immediately shut down its network to prevent further damage.
2. The company paid the ransom, but the attackers failed to provide the decryption key.
3. TechCorp implemented a comprehensive cybersecurity plan, including regular software updates, employee training, and robust backup systems.

- | | | |
|-----|---|-----------|
| (a) | What steps could TechCorp have taken to prevent the ransomware attack? | 07 |
| (b) | How can organizations ensure business continuity in the face of a cyber attack? | 07 |

OR

- | | | |
|------------|---|-----------|
| Q.5 | (a) What are the ethical implications of paying ransom to cyber attackers? | 07 |
| | (b) What role should employee education and awareness play in preventing similar cyber attacks in the future? | 07 |
