

GUJARAT TECHNOLOGICAL UNIVERSITY
MBA SEMESTER- IV - EXAMINATION-SUMMER-2024

Subject Code: 4549251

Date: 26/04/2024

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.

		Marks
Q.1	Definitions / terms / explanations / short questions based on concepts of theory/practical	14
	(a) Email-Spoofing	
	(b) Salami Attack	
	(c) Password Sniffing	
	(d) Cyberterrorism	
	(e) Netizen	
	(f) Web jacking	
	(g) Data Diddling	
Q.2	(a) Explain various categories of cybercrime along with examples.	07
	(b) Discuss global perspectives on Cybercrime.	07
	OR	
	(b) Describe in detail the amendments made in IT Act 2000.	07
Q.3	(a) What is IT governance? Discuss its importance and benefits	07
	(b) Explain Active and Passive attacks.	07
	OR	
Q.3	(a) Discuss the various stakeholders in IT Governance and their performance measurement.	07
	(b) Explain Smishing and Vishing attack in detail.	07
Q.4	(a) What is Phishing? Explain various types of phishing.	07
	(b) How do you ensure a smooth implementation for IT Governance?	07
	OR	
Q.4	(a) Discuss the concept of Identity theft. Discuss countermeasures that can be taken during phishing.	07
	(b) Comment on the statement- 'Incident handling: An Essential Component of Cyber Security'.	07

Q.5**CASE STUDY:**

A 10-person consulting firm sent a small team to South America to complete a client project. During their stay, an employee used a business debit card at a local ATM. A month after returning to the US, the firm received overdraft notices from their bank. They identified fraudulent withdrawals of \$13,000, all originating from South America. There was an additional \$1,000 overdraft fee.

Realizing they had been defrauded, the firm contacted their bank and closed the impacted account immediately. Their attempts to pursue reimbursement from the bank were unsuccessful. The commercial account used at the ATM for local currency had different protections from consumer accounts and the bank was not required to reimburse them for their losses. The bank went on to deduct the \$1,000 overdraft fee from the firm owner's personal account. The entire cash reserve for the small business was wiped out, netting losses of almost \$15,000.

The firm severed ties with that bank. The firm connected with a new bank. The new bank offered comprehensive fraud protection guarantees. The firm created two business accounts: one for receiving funds and making small transfers and another one for small expense payments. The firm updated travel protocols, banning the use of company-provided debit cards. Employees now prepay expenses electronically, pay cash, or use a major credit card, as necessary.

- (a)** Discuss in detail the attack that has been carried out in the case? **07**
- (b)** Knowing how the firm responded, what would you have done differently? **07**

OR

- Q.5 (a)** The firm in the case has moved to electronic transaction or credit card. Discuss Organization Security policies and Measures for Credit cards for such a firm. **07**
- (b)** What are some steps you think the firm could have taken to prevent this incident? **07**
