Scenario	Asset	Threat	Vulnerability	Attack	Control
1. Public Wi-Fi Access	Company internal system & financial data	Unauthorized access	Use of unsecured public Wi-Fi	Man-in-the-middle attack leading to fraudulent transactions	Enforce VPN use Multi-factor authentication and security awareness training
2. Fake HR Email	Employee login credentials	Phishing	Lack of email verification awareness	Credential harvesting via malicious link	Email filtering phishing awareness training MFA
3. Fake Tech Support Call	Employee credentials	Social engineering	Trust in authority figures	Impersonation attack (pretexting)	Verification protocols employee training, caller ID Validation
4. Fake Login Page	User credentials & financial data	Credential theft	Weak URL verification	Pharming attack (redirect to fake site)	Anti-Phishing tools, SSL/TLS enforcement, user awareness
5. Power Interruption	Company servers & stored data	Data corruption	Lack of backup/power redundancy	Improper shutdown causing data loss	UPS systems, regular backups, disaster recovery plan
6. Malicious Attachment	Employee workstation & files	Malware infection	Opening unverified attachments	Ransomware attack (file encryption)	Email attachment scanning, endpoint protection, user training

7. Stolen Laptop	Sensitive customer data	Physical theft	Lack of encryption & physical security	Data breach via stolen device	Full-disk encryption, remote wipe capability, physical security policies

1. What would happen to the organization if no security controls were implemented?

Answer : Without security controls, the organization would face frequent breaches, data loss, financial fraud, and reputational damage. Employees and customers would lose trust, and regulatory penalties could be imposed for failing to protect sensitive information. Ultimately, the business could suffer severe operational disruption or even collapse.

2. Why must management and IT work together in information security?

Answer : Management sets policies, allocates resources, and enforces compliance, while IT implements technical safeguards and monitors threats. Collaboration ensures that security measures align with business goals and that employees are properly trained. A united approach creates a culture of security, reducing risks and strengthening resilience against attacks.