Name: Ngoc Phuong Trang Duọng
ID: 223990468

Task 10.1P: Database Security

Question 1:

1. **Weak password practices:** Most employees use their birth year in passwords, and in some cases, IT Support Manager advised staff to set short passwords. This makes passwords easy to guess and vulnerable to brute-force attacks.
2. **Use of personal USB drives:** Senior accountant backs up client records on his personal flash drive. This exposes sensitive data to loss or theft outside the company's control.
3. **Lack of endpoint protection:** Remote access is allowed for directors who do not use VPNs. This enables potential interception of data over unsecured public networks.
4. **No VPN for remote access:** Main computer used for transactions hasn't been updated recently but is still in use. Outdated systems are more likely to contain unpatched vulnerabilities.
5. **Susceptibility to phishing:** An email pretending to be from Ms. Carter asked staff to verify credentials, several complied without checking the source. This shows poor employee awareness and lack of verification protocols.

Question 2: Three security measures to prevent data breaches in the event of device loss or theft.

1. **Full Disk Encryption**
   Encrypt all data stored on devices so that even if stolen, the data cannot be accessed.
2. **Remote Wipe Capability**
   Use mobile device management (MDM) to remotely wipe lost or stolen laptops or smartphones.
3. **Device Access Controls**
   Require strong passwords, biometric login, and automatic screen lock after inactivity to prevent unauthorized access.

Question 3:

1. **Email Authentication Protocols (SPF, DKIM, DMARC)**: Ensure all company emails are verified using email authentication standards to prevent spoofing.
2. **Staff Cybersecurity Training**: Educate staff on phishing techniques, red flags (e.g., urgent language, odd sender addresses), and how to report suspicious messages.
3. **Multi-step Verification Process**: Any email requesting credentials or sensitive actions should be verified via a secondary method (e.g., phone call or internal chat).

Question 4:

1. **Secure Cloud Storage**: Use secure and encrypted cloud services (e.g., OneDrive for Business, Google Workspace) that support access control and audit logs.

2. **Encrypted Company-Issued Devices**: Provide employees with encrypted laptops where data storage and access is centrally controlled.
3. **VPN Access to Internal Network**: Allow remote access through secure VPNs to access files without copying them to external devices.

Question 5:

In March 2023, Latitude Financial Services, a leading consumer finance company in Australia, confirmed one of the largest data breaches in the country's financial sector. The cyberattack resulted in the exposure of data from over 14 million customers, including highly sensitive personal information such as driver's licenses, passports, contact details, dates of birth, and account information.

Initially, Latitude reported that around 300,000 customer records were affected. However, after further investigation, the actual number turned out to be much higher. Among the 14 million records, a significant portion dated back over ten years, including data from former customers who no longer had any relationship with the company.

This incident was not only significant in terms of the number of records breached but also highlighted the company's failure to manage data lifecycle properly — especially in retaining, protecting, and deleting old customer information according to best practices.
The breach began when hackers gained access to login credentials belonging to a third-party service provider's employee. Using this access, the attackers infiltrated Latitude's internal systems and browsed and extracted vast amounts of sensitive customer data, which could be used for identity theft and fraud.

Latitude confirmed that there was no evidence the stolen data was encrypted, making it easier for the attackers to copy and misuse the information. Additionally, the absence of multi-factor authentication (MFA) and inadequate access control mechanisms allowed the breach to escalate. Worryingly, Latitude did not detect the breach immediately. It was only made aware of the incident by the third-party vendor. This delay reflects serious weaknesses in the company's monitoring and threat detection systems, which failed to identify abnormal activities or targeted attacks in real time.

Consequences for skateholder is
Customers
Millions of customers were seriously affected. Many were concerned about identity theft, unauthorised financial transactions, and the emotional stress caused by the breach. They felt betrayed, especially those who had ceased using Latitude's services years ago but still had their personal data stored without valid reasons.
Latitude offered free credit monitoring services to affected customers. However, this measure did little to relieve the public's anxiety or rebuild trust.
Latitude Financial
The company faced severe damage to its reputation, customer confidence, and significant financial losses due to legal costs, customer compensation, and regulatory scrutiny. A class-action lawsuit was launched on behalf of the victims seeking justice and redress.

Latitude also came under investigation by regulatory bodies such as the Office of the Australian Information Commissioner (OAIC) for potential violations of data privacy regulations and failure to follow adequate security protocols.

Regulators and the industry

The breach prompted regulatory bodies like OAIC, ACCC, and the Australian Government to review existing data protection regulations, especially regarding how long companies are allowed to retain customer data.

The incident served as a wake-up call for the entire financial industry and all data-heavy businesses in Australia. It emphasized the increasing public demand for data transparency, digital responsibility, and customer rights in the digital age.

To prevent this accident, this company should:

1. Enforce strong multi-factor authentication (MFA)

MFA is a crucial safeguard against unauthorized access. Even if login credentials are compromised, attackers cannot proceed without a second authentication factor, such as a one-time code or biometric verification.

2. Encrypt all sensitive data

Personally identifiable information such as IDs, licenses, and passports should be protected using robust encryption (e.g., AES-256) both at rest and in transit, preventing it from being readable if accessed unlawfully.

3. Implement strict data lifecycle management

Companies should establish clear data retention and deletion policies. Outdated customer data that is no longer necessary must be deleted or anonymized to reduce risk.

4. Improve monitoring and early detection systems

Tools such as Intrusion Detection/Prevention Systems (IDS/IPS), user activity monitoring, and audit logs should be implemented to detect suspicious behavior and respond quickly.

5. Train employees and third-party vendors

Cybersecurity awareness training is essential for both internal staff and third-party vendors. They must be equipped to recognize phishing, social engineering, and insider threats, and understand proper data handling procedures.

In conclusion, the Latitude Financial breach was not just an isolated security incident but a critical lesson for all businesses handling sensitive data. In a world where data is one of the most valuable assets, cybersecurity is not optional — it is mandatory.

To avoid similar events in the future, companies must combine technological safeguards, internal procedures, and a culture of security awareness across the entire organization. Only then can businesses earn and maintain customer trust and operate safely in today’s digital environment.