Ngoc Phuong Trang Duong – s223990468
Deakin University

Question 1:

1. **Weak password practices:** Most employees, including senior staff and interns, use their birth year as passwords, and IT Support Manager Robert Hale even advises setting short passwords to avoid lockouts. This practice makes accounts vulnerable to brute-force attacks and password guessing, especially for the financial database.
2. **Use of personal USB drives:** Senior accountant Mark Dawson frequently backs up client financial records on his personal USB drive to work from home, which risks unauthorized access and potential data loss or theft.
3. **Lack of endpoint protection:** The company allows directors Sarah Whitmore and James Reynolds to access the primary financial database remotely without using VPNs, increasing the risk of interception over unsecured networks.
4. **Outdated system without security updates:** One of the main computers used for financial transactions has not been updated recently. Despite its continued functionality, this exposes it to known vulnerabilities and exploits.
5. **Susceptibility to phishing attacks:** An email appearing to be from Ms. Carter tricked several staff into providing login credentials. This indicates a lack of verification protocols and employee awareness regarding phishing attempts.

Question 2:

1. **Full disk encryption:** Encrypt all data stored on devices, ensuring that stolen or lost devices do not expose sensitive information. For example, the laptop stolen during the office break-in should have been encrypted to protect client data.
2. **Remote wipe capability:** Implement a mobile device management (MDM) system to remotely wipe data on lost or stolen devices, such as the missing company laptop. This minimizes the risk of data breaches.
3. **Device access controls:** Mandate strong passwords, biometric authentication, and automatic screen locks on all devices. These controls reduce the chance of unauthorized access if a device is misplaced or stolen.

Question 3:

1. **Email authentication protocols (SPF, DKIM, DMARC):** Configure the company's email systems to automatically reject unauthenticated emails, reducing the chance of email spoofing like the Ms. Carter phishing incident.

2. **Employee training on phishing awareness:** Conduct regular cybersecurity awareness training for employees, emphasizing red flags (e.g., unexpected requests, urgency, or suspicious sender addresses). In the Ms. Carter case, training would have prepared staff to recognize the phishing attempt.
3. **Multi-step verification process:** Require a secondary verification method such as phone calls or internal messaging, for any email requesting credentials or sensitive data. This would have prevented staff from blindly trusting the fraudulent email.

Question 4:

1. **Secure cloud storage:** Provide employees with access to encrypted cloud storage solutions (e.g., OneDrive for Business or Google Workspace) that include audit trails and access controls. This eliminates the need for USB drives.
2. **Encrypted, company-issued laptops:** Assign encrypted laptops to staff handling sensitive data, including Mark Dawson, ensuring that information remains secure and centrally managed.
3. **VPN access to the internal network:** Allow employees to work remotely using secure VPNs to access internal files directly, avoiding the need to transfer sensitive data to personal devices.

Question 5:

In March 2023, Latitude Financial Services, a major consumer finance company in Australia, experienced one of the largest data breaches in the country's history. Hackers accessed the data of over 14 million customers, including highly sensitive information such as driver's licenses, passports, and financial details.

The breach began when cybercriminals obtained login credentials from a third-party service provider's employee. This allowed them to infiltrate Latitude's internal systems and extract data. The attack was facilitated by the absence of multi-factor authentication (MFA), lack of encryption for stored data, and inadequate access controls. Alarmingly, Latitude did not detect the breach itself but was notified by the third-party vendor, highlighting deficiencies in its monitoring and detection systems.

The consequences were severe:

- Customers faced identity theft risks, unauthorized financial transactions, and emotional distress. Many were especially angered by the inclusion of outdated records from years past.
- Latitude suffered reputational damage, regulatory investigations by OAIC and ACCC, and financial losses from compensation and lawsuits.

- Regulators tightened scrutiny of data protection laws, prompting the entire financial sector to reassess data handling practices.

Preventive measures that could have avoided the breach include:

- Implementing strong MFA: Would have blocked unauthorized access even if login credentials were compromised.
- Encrypting sensitive data: Would have rendered stolen data unreadable, reducing the impact of the breach.
- Establishing clear data lifecycle policies: Deleting or anonymizing outdated customer data reduces the risk of unnecessary exposure.
- Enhancing threat monitoring and detection systems: Could have identified abnormal activities in real time, mitigating the breach's scope.
- Providing comprehensive cybersecurity training: For both employees and third-party vendors to recognize and mitigate phishing and insider threats.

In today’s rapidly evolving digital landscape, database security is no longer optional, it is a fundamental requirement. The case of Sunrise Financial Solutions reveals common yet critical vulnerabilities that many growing businesses face, such as weak password policies, insecure data handling practices, and a lack of employee training. By drawing lessons from the Latitude Financial Services data breach, Sunrise and indeed any organization, can see the real-world consequences of neglecting robust security measures. Proactive steps such as enforcing strong authentication, encrypting sensitive data, implementing secure data lifecycle management, and providing comprehensive employee training are essential to protect valuable customer information. Beyond technology, fostering a culture of security awareness is equally vital, ensuring that all staff understand their role in safeguarding data. Ultimately, investing in database security not only protects a company’s reputation and finances but also strengthens customer trust, an invaluable asset in the digital era.