Deakin University

Database Fundamentals

OnTrack Submission

Database security

Submitted By:
Prakhar Pandey
s223638985
2025/05/19 02:33

Tutor:
Mohammad belayet Hossain

Outcome	Weight
Fundamental concepts of database	♦♦♦♦♦
Relational Database Modelling	♦♦♦♦♦
Structured Query Language (SQL)	♦♦♦♦♦
Reflection	♦♦♦♦♦
Research and critical review	♦♦♦♦♦

This submission addresses real-world database security issues and aligns with SIT772 outcomes by applying core principles to both a scenario analysis and a relevant Australian data breach case.

May 19, 2025

Produced by Doubtfire

Sunrise Financial Solutions

Task 1. List five security vulnerabilities present in Sunrise Financial Solutions' operations. Provide evidence from the scenario to support your answer.

1. Weak and Predictable Password Practices

One of the most prominent security vulnerabilities at Sunrise Financial Solutions is the widespread use of weak and easily guessable passwords. According to the scenario, many employees create passwords using their birth year, and in some cases, the IT Support Manager, Robert Hale, has even encouraged staff to set short passwords to avoid being locked out. This practice significantly reduces the strength of account authentication and exposes the organization to brute-force and dictionary attacks. Predictable passwords are one of the leading causes of unauthorized access to systems, especially when there is no multi-factor authentication in place. Encouraging short or simplistic passwords reflects a poor security culture and an absence of policy enforcement around credential hygiene.

2. Use of Personal and Unsecured USB Devices

The firm also suffers from unsafe data handling practices, particularly with portable storage. The scenario describes how Senior Accountant Mark Dawson backs up confidential client financial records onto his personal flash drive to work from home. Additionally, interns and junior staff frequently exchange files using USB drives to speed up workflow. While convenient, these methods pose serious risks. Personal USB drives may lack encryption, can be easily lost or stolen, and provide an uncontrolled medium for transferring sensitive data. Moreover, such devices can act as vectors for malware, putting the firm's entire network at risk if they are plugged into office systems without proper scanning or access control.

3. Unpatched and Outdated Systems

Another significant vulnerability arises from the organization's failure to maintain up-to-date software on its systems. One of the main computers used for financial transactions has reportedly not received recent security updates. Despite this, no action has been taken because the system continues to function smoothly. This reactive approach to IT management is dangerous. Failing to apply timely security patches leaves systems exposed to known vulnerabilities, many of which are documented and exploited by cybercriminals. This could lead to data breaches, ransomware attacks, or system manipulation, especially given the sensitive nature of financial and tax information stored in the firm's databases.

4. Remote Access Without Secure VPN Usage

Remote access by the firm's directors, Sarah Whitmore and James Reynolds, represents another critical point of weakness. While remote access itself is not inherently insecure, the directors deliberately avoid using a Virtual Private Network (VPN), citing concerns about efficiency. VPNs are designed to encrypt data in transit and protect sensitive information from interception over unsecured or public networks. Without a VPN, any remote connection could be hijacked, especially if accessed from a compromised or poorly secured device or network. This behaviour undermines the integrity of the firm's data access protocols and puts confidential client information at unnecessary risk.

5. Susceptibility to Phishing Attacks

Finally, Sunrise Financial Solutions demonstrates a lack of preparedness in identifying and responding to phishing threats. The scenario mentions an incident where several staff members received a fraudulent email that appeared to be from Ms. Carter, requesting them to verify their credentials for an internal update. Employees complied without verifying the legitimacy of the request. This illustrates a major gap in both technical safeguards and employee training. There appear to be no authentication mechanisms, such as digital signatures, or policies requiring verification of sensitive email requests. As a result, the organization is vulnerable to credential theft, unauthorized access, and further social engineering attacks.

Task 2. Outline three security measures that should be implemented to prevent data breaches in the event of device loss or theft?

1. Full-Disk Encryption
One of the most effective ways to protect sensitive information stored on laptops or other devices is to implement full-disk encryption. This security measure ensures that all data on a device is automatically encrypted, making it unreadable without proper authentication credentials. Even if the physical device is lost or stolen as was the case with the company-issued laptop at Sunrise Financial Solutions the data remains secure and inaccessible to unauthorized users. Tools such as BitLocker (Windows) or FileVault (macOS) are widely used for this purpose and can be centrally managed by an organization's IT team to enforce encryption across all employee devices. Encryption acts as a final safeguard, ensuring that even when a breach of physical security occurs, digital security remains intact.

2. Remote Device Management and Wipe Capability
Another critical safeguard against data loss is the ability to remotely manage and wipe lost or stolen devices. Using endpoint management solutions like Microsoft Intune, Jamf, or similar tools, organizations can track devices, enforce security policies, and remotely erase all data from the system. In the context of Sunrise Financial Solutions, where a laptop used to handle client information was stolen during a break-in, the absence of such a capability represents a serious oversight. Had remote wipe functionality been enabled, the IT team could have immediately erased sensitive files and deactivated system access, thereby mitigating the risk of a data breach. Additionally, device location tracking may assist in recovery efforts and inform authorities during an investigation.

3. Multi-Factor Authentication (MFA)
While encryption and remote wipe capabilities protect stored data, access control must also be reinforced to prevent unauthorized logins. Multi-Factor Authentication (MFA) is a widely adopted measure that adds an extra layer of security to device and account access by requiring two or more forms of verification—such as a password plus a fingerprint or one-time code sent to a mobile device. If MFA had been implemented at Sunrise Financial Solutions, even if someone gained physical access to the stolen laptop, they would not be able to log in without the second authentication factor. MFA significantly reduces the likelihood of unauthorized access, especially when combined with strong password policies and secure device configurations.

These three measures: encryption, remote wipe capabilities, and MFA, work best when used together as part of a holistic device security policy. Implementing them not only protects sensitive financial data but also demonstrates organizational due diligence in compliance with data protection regulations and cybersecurity best practices.

Task 3. What measures should be in place to verify the authenticity of internal emails requesting sensitive information, considering that staff members complied without double checking the source when an email appearing to be from Ms. Carter requested employees to verify their credentials for an internal update? Provide three measures.

1. Implement Email Authentication Protocols (SPF, DKIM, DMARC)
One of the most effective technical measures to prevent email spoofing is to implement industry standard email authentication protocols such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance). These protocols validate the sender's identity and ensure that emails are genuinely sent from authorized servers. If Sunrise Financial Solutions had implemented such mechanisms, the spoofed email that appeared to come from Ms. Carter would likely have failed validation and either been flagged as suspicious or blocked before reaching employees' inboxes. These protocols also provide IT administrators with reports on failed email deliveries, enabling proactive threat monitoring.

2. Establish a Clear Internal Verification Policy
Even with technical safeguards in place, human error remains a major vulnerability. Organizations should implement and enforce a formal policy that requires all staff to verify the authenticity of internal emails before acting on requests involving credentials, financial data, or confidential files. This policy should mandate that employees confirm such requests through a second communication channel such as a phone call, in person conversation, or internal messaging system like Slack or Microsoft Teams. In the case of Sunrise Financial Solutions, staff members should have been required to confirm the identity of the sender before inputting their credentials in response to the email. A simple internal check could have prevented the compromise.

3. Conduct Regular Phishing Awareness Training and Simulations
Cybersecurity awareness training is essential to building a vigilant and informed workforce. Employees should be trained to recognize common phishing tactics, such as urgency, impersonation, or unusual file attachments. More importantly, organizations should conduct simulated phishing campaigns to test staff response and identify gaps in awareness. Had Sunrise Financial Solutions implemented ongoing phishing simulations, staff may have been more cautious and less likely to trust the fraudulent email from “Ms. Carter.” These exercises also help reinforce a “security-first” mindset across the organization and improve long-term employee behaviour around email hygiene.

Together, these three measures- email authentication protocols, a strong internal verification policy, and phishing awareness training form a multi-layered defense against social engineering attacks. Implementing them would greatly reduce the likelihood of staff falling for spoofed or malicious internal emails, as happened in this scenario.

Taks 4. What are three safer alternatives to minimize the security risks associated with storing client financial records on personal USB drives?

1. Use of Secure, Encrypted Cloud Storage Services
One of the most secure and scalable alternatives to USB drives is the use of encrypted cloud storage platforms such as Microsoft OneDrive for Business, Google Drive (Enterprise edition), or Dropbox Business. These platforms offer advanced security features including role-based access control, file-level encryption, real-time syncing, and automatic backups. By storing client financial records in the cloud, Sunrise Financial Solutions can ensure that data is accessible only to authorized users and is protected from physical loss or unauthorized duplication. Additionally, cloud services enable IT administrators to track access history and revoke permissions instantly if needed—something that is impossible with personal USB devices.

2. Deployment of Enterprise-Grade Encrypted External Drives
If offline access is essential due to fieldwork or travel, staff can be provided with company-issued encrypted external hard drives or secure USB drives. These devices often include hardware-level encryption, password protection, and automatic data wiping after multiple failed login attempts. Unlike personal USBs, enterprise-grade secure drives (e.g., IronKey or Kingston DataTraveler Vault) are designed with regulatory compliance and business use in mind. For example, data stored on these devices can be protected using AES-256 encryption and integrated with IT asset management software for tracking. This allows employees like Mark Dawson to work remotely without compromising data security.

3. Implementing VPN-Based Remote Access to Internal File Systems
Another safer alternative is to enable employees to access internal systems and file servers remotely through a secure Virtual Private Network (VPN). VPNs create an encrypted tunnel between the user and the organization’s network, allowing employees to work from anywhere without copying files onto external devices. Combined with access control policies and endpoint protection, VPNs provide a secure environment for accessing sensitive client information. In the case of Sunrise Financial

Solutions, adopting VPN-based access would eliminate the need for interns or senior accountants to physically carry sensitive data, reducing the risk of loss or data leakage.
By replacing personal USB drives with secure cloud storage, encrypted hardware, or VPN-enabled remote access, Sunrise Financial Solutions can greatly improve the security of client financial records while maintaining productivity and flexibility for its staff.

Task5: Choose a recent data breach incident that has been reported in the media and write a concise essay.

Case Study: Optus Data Breach (2022)

What Happened?

In September 2022, Optus, Australia's second-largest telecommunications provider, suffered a massive data breach that exposed the personal information of approximately 9.8 million current and former customers. The stolen data included names, dates of birth, phone numbers, email addresses, and, in many cases, sensitive identification documents such as driver's licence and passport numbers. The breach quickly became one of the most significant cybersecurity incidents in Australian history, given both the scale of the impact and the sensitivity of the data exposed.
Optus publicly confirmed the breach on September 22, 2022, and immediately notified affected customers, the Australian Cyber Security Centre (ACSC), and the Office of the Australian Information Commissioner (OAIC). The incident prompted swift government and public scrutiny and led to widespread concern about data security across Australia's critical infrastructure sectors.

How Did It Happen?

The breach occurred due to a vulnerability in an unauthenticated API endpoint that was accessible via the internet. This misconfigured API did not require login credentials and allowed the attacker to query customer records directly. The hacker exploited this weakness to extract millions of customer records without triggering any authentication or access control mechanisms.
Reports suggested that the breach was not the result of a sophisticated cyberattack but rather a basic misconfiguration and lack of oversight. Security experts criticised Optus for failing to apply industry-standard security practices such as access authentication, rate limiting, and API monitoring. The attacker reportedly contacted Optus with a ransom demand, threatening to release the data unless payment was made. However, the ransom demands were later withdrawn, and the attacker claimed to have deleted the data.

Consequences for Stakeholders

- **Customers**: The breach exposed millions of individuals to identity theft, fraud, and phishing attacks. Many were required to replace their driver's licences and passports. Emotional distress and anxiety over potential misuse of personal information were also reported.
- **Optus**: The company faced intense reputational damage, class action lawsuits, and regulatory investigations. Optus had to fund the cost of ID document replacements and provide identity protection services to affected customers. The incident also disrupted its customer trust and brand equity.
- **Government and Regulators**: In response, the Australian government moved quickly to review privacy laws, including introducing legislation to increase penalties for serious data breaches and allowing better data sharing with government agencies during incidents. Regulatory bodies like OAIC and the Australian Communications and Media Authority (ACMA) launched formal investigations into Optus' compliance with data protection obligations.
- **Broader Industry**: The breach acted as a wake-up call for other organisations across Australia, especially those in telecommunications, finance, and healthcare. It triggered renewed focus on API security, data minimisation, and third-party risk management.

How Could It Have Been Prevented?

1. **API Authentication and Access Control**: The core issue was that a public-facing API lacked authentication requirements. Properly securing APIs through access tokens, user authentication, and role-based access would have blocked the attack.
2. **Regular Security Audits and Penetration Testing**: Routine vulnerability assessments and penetration tests could have revealed the misconfigured API endpoint before it was exploited. Internal red team exercises may also have helped uncover risky configurations.
3. **Rate Limiting and Monitoring**: The attacker made numerous API queries to extract data. Implementing rate limiting and anomaly detection systems could have triggered alerts about the unusual access pattern.
4. **Data Minimisation Practices**: Optus stored large volumes of sensitive data for both current and former customers. Implementing strict data retention policies and anonymising non-active user data would have limited the scope of the breach.
5. **Incident Response Readiness**: While Optus was quick to disclose the breach publicly, the company appeared unprepared in terms of customer communication, government engagement, and containment strategies. Developing a detailed incident response plan with assigned roles and decision trees would improve future response effectiveness.
6. **Zero Trust Security Framework**: Applying the principles of zero trust, such as "never trust, always verify," across systems and APIs would require authentications for all endpoints, preventing such unauthenticated access.

The Optus breach highlights that even large and well-resourced organisations can fall victim to basic security oversights. It underscores the critical importance of secure system configurations, continuous monitoring, and regulatory compliance in protecting personal data in the digital era.

Reference:

1) Optus Sept 2022 cyber-attack/data leak - Optus Broadband. (2022, September 21). Whirlpool.net.au; Whirlpool. https://forums.whirlpool.net.au/archive/3z4yl2qw

2) OAIC. (2023, March 10). OAIC updated statement on Optus data breach. OAIC. https://www.oaic.gov.au/news/media-centre/oaic-updated-statement-on-optus-data-breach