Security Risk Assessment Report for Medibank

1.0. Executive Summary

In October 2022, Medibank, one of Australia's largest health insurers, experienced a cyber breach compromising 9.7 million customer records (UpGuard, 2024). Exposed data included personally identifiable information (PII) such as names, birthdates, passport numbers, and Medicare claim details.

This breach led to:

- Regulatory scrutiny under the Australian Privacy Act, APRA CPS 234, and GDPR.
- Severe reputational damage, leading to customer trust erosion.
- Potential financial and legal consequences, including penalties and class-action lawsuits.

This report assesses Medibank's current security posture, identifying key vulnerabilities, accordingly recommending risk mitigation strategies aligned with ISO 27001, PCI DSS, and GDPR.

2.0. Identified Vulnerabilities

Upon inspection of Medibank's current security posture, the following vulnerabilities were identified. These vulnerabilities, in combination with the actions of a cyberattacker, pose risk to Medibank's systems:

- **Multi-Factor Authentication (MFA) is not used.** MFA adds another step in the authentication process of all employees, and is strongly recommended by *ISO 27001* standards.
- **A lack of cyber awareness amongst employees**. Most data breaches involving compromised employee credentials, originate upon the attacker successfully retrieving details from the employee. This is mostly from techniques such as phishing, which involves the attacker sending fraudulent emails with malicious links to unaware employees with malicious links, leading to credential-stealing websites.
- **DNSSEC is not enabled.** DNSSEC records prevent third parties from forging the records that guarantee a domain's identity.

3.0 Risk Mitigation Strategies & Implementation Plan

3.1. Implement Multi-Factor Authentication (MFA) for All Employees

- **Issue:** Medibank lacked MFA, making credential theft easier.
- **Recommendation:** Implement phishing-resistant MFA (e.g., *FIDO2 security keys* instead of *SMS-based OTPs*).
- **Implementation Plan:**
    - Enforce MFA across all employee and administrator accounts.

    - Integrate MFA logs into **SIEM tools** (*Splunk, Chronicle, Azure Sentinel*) to monitor login anomalies.

- **Compliance Alignment:** *ISO 27001 A.9.4.1, NIST 800-63B, APRA CPS 234.*

3.2. Establish Mandatory Cybersecurity Awareness Training

- **Issue:** Employees were targeted via phishing, leading to credential compromise.

- **Recommendation:** Implement quarterly **phishing simulations and security awareness training**.

- **Implementation Plan:**
    - Conduct mandatory employee training on phishing indicators and social engineering threats.
    - Simulate phishing attacks and track user response rates to assess risk levels.

- **Compliance Alignment:** *ISO 27001 A.7.2.2, NIST CSF PR.AT-1, GDPR Article 32.*

3.3. Enforce the Principle of Least Privilege (POLP) & Access Control Measures

- **Issue:** Excessive access permissions allowed attackers to escalate privileges.

- **Recommendation:** Implement Role-Based Access Control (RBAC) and enforce Just-In-Time (JIT) access management.

- **Implementation Plan:**
    - Conduct audits to identify set privileges and remove unnecessary access rights.
    - Implement segregation of duties to prevent unauthorised data access.

- **Compliance Alignment:** *ISO 27001 A.9.1.2, A.9.2.3, NIST SP 800-53 AC-6.*

3.4. Implement Network Segmentation

- **Issue:** Lack of segmentation allowed unrestricted attacker movement across the network.

- **Recommendation:** Isolate sensitive data and critical systems into separate security zones.

- **Implementation Plan:**
  - Deploy firewalls & VLANs to restrict unauthorised access between departments.
  - Implement Zero Trust Network Access (ZTNA) to verify users before granting access.

- **Compliance Alignment:** *PCI DSS Requirement 11.3, GDPR Article 25, ISO 27001 A.13.1.3.*

4.0. Conclusion and Next Steps

By implementing these risk mitigation strategies, Medibank can:

- Enhance cybersecurity resilience against credential-based attacks.
- Meet compliance requirements under *ISO 27001, PCI DSS, GDPR, and APRA CPS 234*.
- Reduce the likelihood of future breaches by improving access controls, network security, and employee training.

4.1. Immediate Action Plan

1. Initiate an *ISO 27001* internal audit to assess current gaps.
2. Deploy MFA and access control policies within the next 3 months.
3. Conduct phishing simulation tests within 6 months to measure training effectiveness.
4. Segment critical systems and enforce Zero Trust policies by end of year.

5.0 References

- UpGuard (2024). *What caused the Medibank breach?* https://www.upguard.com/blog/what-caused-the-medibank-data-breach

- Australian Cyber Security Centre (2023). *Essential Eight assessment procedure guide.* https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/e ssential-eight/essential-eight-assessment-process-guide

- APRA CPS 234 (2019). *Prudential Standard CPS 234 Information Security.* https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf