Risk Register Assessment

Dear Management,

Provided is the risk register assessment for Medibank, based on their 2024 Annual Report.

Best Regards,

Yasif Farook

Junior Cyber-Risk Consultant

Operational environment:

Medibank's Sydney office is located in the busy, central business district area with low crime rates. Many people and systems handle the company data—3568 total employees (*Annual Report*, 2024). The customer base of the bank includes 4.2 million accounts, consisting of both individual users and commercial base. The bank's services are marketed by the AFL Women's league, who have established themselves as an official health sponsor. Medibank employs a centralised marketing approach to promote its services, ensuring efficiency and agility. By consolidating their marketing operations, they aim to optimise resources and minimise risks. Medibank operates under stringent financial regulations, complying with standards set by the Australian Prudential Regulation Authority (APRA). Their Corporate Governance Statement outlines adherence to these regulations, ensuring sound corporate practices and financial integrity. Since the 2022 data breach, Medibank has complied with ISO 27001 standards, alongside Consolidated Prudential Standard 220 Risk Management("CPS220") standards. As a private healthcare company, Medibank must also comply with the Australian Privacy Act 1988, and the Australian Privacy Principles (APPs) for protecting patient data.

Asset	Risk(s)	Description (Threat + Vulnerability)	Likelihood	Severity	Priority
Customer Data	Unauthorised Access and Data Breach	*Phishing + Lack of MFA -> Hackers steal credentials and access data.*	3	3	9
Employee Accounts	Credential Theft and Social Engineering	*Phishing + Lack of Cyber Awareness -> Employees unknowingly provide access.*	3	3	9
Network Infrastructure	Lateral Movement & Widespread Data Access	*No Network Segmentation -> Attackers move freely after breaching one system.*	3	3	9
Internal IT Systems	Privilege Escalation and Insider Threats	*Overprivileged accounts (No POLP) -> Hackers gain unrestricted access.*	3	3	9
Public-Facing Website	Domain Spoofing and MITM Attacks	*Fake login pages + Lack of DNSSEC ⟶ Attackers steal customer credentials.*	2	3	6
Notes	*How are security events possible considering the risks the asset faces in its operating environment?* Security events are possible in Medibank's operational environment due to specific vulnerabilities and the contextual factors influencing each asset's exposure to risks.				

Justifications for Risk Ratings:

1. **Customer Data:** Unauthorised Access and Data Breach **(9)**

Phishing is a common attack method. Medibank holds millions of customer records, making it a high-value target. Lack of MFA heightens the likelihood of this risk. Breaches violate *APRA CPS 234* and the *Privacy Act*, risking fines, lawsuits and reputational harm.

2. **Employee Accounts:** Credential Theft and Social Engineering **(9)**

At the forefront, employees are prime targets for cybercrime. Up to 92% of breaches involve human error (*Verizon DBIR*, 2023). Stolen credentials can lead to unauthorised access to internal systems, hence data theft and/or exploitation.

3. **Network Infrastructure:** Lateral Movement and Widespread Data Access **(9)**

Lack of segmentation enables free movement within the network. This allows attackers to escalate access to all customer records, resulting in a catastrophic data leak.

4. **Internal IT Systems:** Privilege Escalation and Insider Threats **(9)**

A compromised account with admin access can lead to a full system compromise. Lack of strict access privileges heightens this risk, and its impact.

5. **Public-Facing Website:** Domain Spoofing and MITM Attacks **(6)**

Successful attacks can lead to credential theft and account compromises. Risk is lower due to domain spoofing requiring greater effort to enact.

Immediate Priorities: Focus on complying with regulations by securing customer data. Avoid falling victim to social engineering by prioritising a cybersmart workforce. Implement *NIST* and *CSF*-approved network policies to limit impact of cyber risks.

Glossary of Terms Used:

Asset: The asset at risk of being harmed, damaged, or stolen.
Risk(s): A potential risk to the organisation's information systems and data.
Description: A vulnerability that might lead to a security incident.
Likelihood: Score from 1-3 of the chances of a vulnerability being exploited. A 1 means there's a low likelihood, a 2 means there's a moderate likelihood, and a 3 means there's a high likelihood.
Severity: Score from 1-3 of the potential damage the threat would cause to the business. A 1 means a low severity impact, a 2 is a moderate severity impact, and a 3 is a high severity impact.
Priority: How quickly a risk should be addressed to avoid the potential incident. Use the following formula to calculate the overall score: **Likelihood x Impact Severity = Risk**

medibank
For Better Health

Sample Risk Matrix

Likelihood	Severity: Low 1	Severity: Moderate 2	Severity: Catastrophic 3
Certain 3	3	6	9
Likely 2	2	4	6
Rare 1	1	2	3