



# Strengthening Medibank's Security & Privacy Posture

Risk Assessment & Mitigation Strategies

By Yasif Farook



# Executive Summary

## What Happened?

The 2022 cyber breach exposed 9.7 million customer records

Regulatory, financial, and reputational damage.

Increased risk of fines, lawsuits, customer trust loss, and stricter regulations.

## What's Next?

This will:

A structured risk mitigation plan

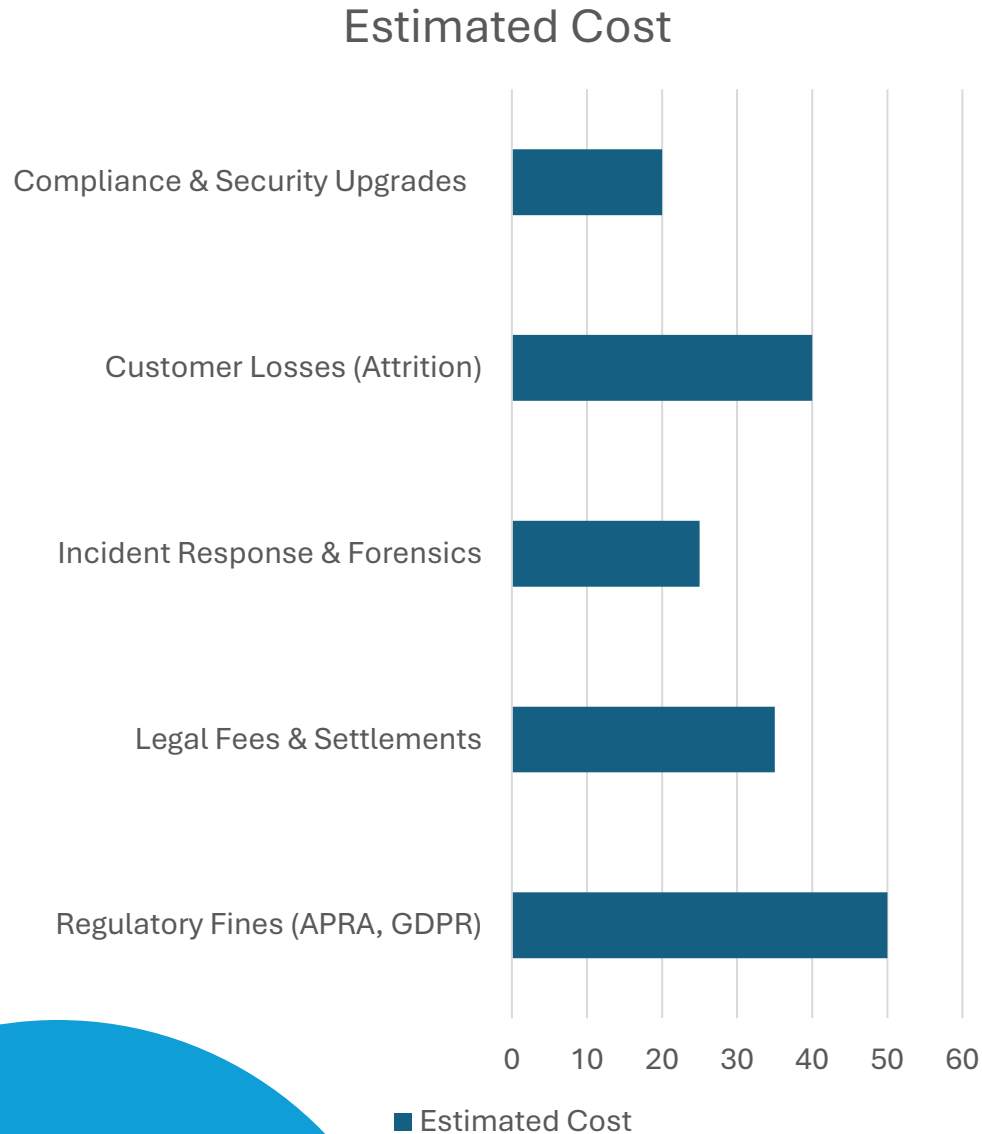


Strengthen security



Prevent future breaches





# Business Impact



💰 **Financial Losses:** Estimated costs in fines, legal fees, and incident response.

⚖️ **Regulatory Scrutiny:** APRA CPS 234, Australian Privacy Act, and GDPR enforcement risks.

🤝 **Customer Trust Impact:** Reputation damage could lead to customer attrition.

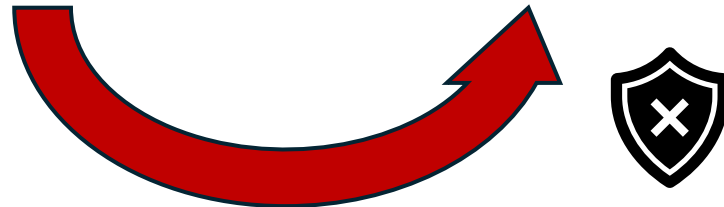
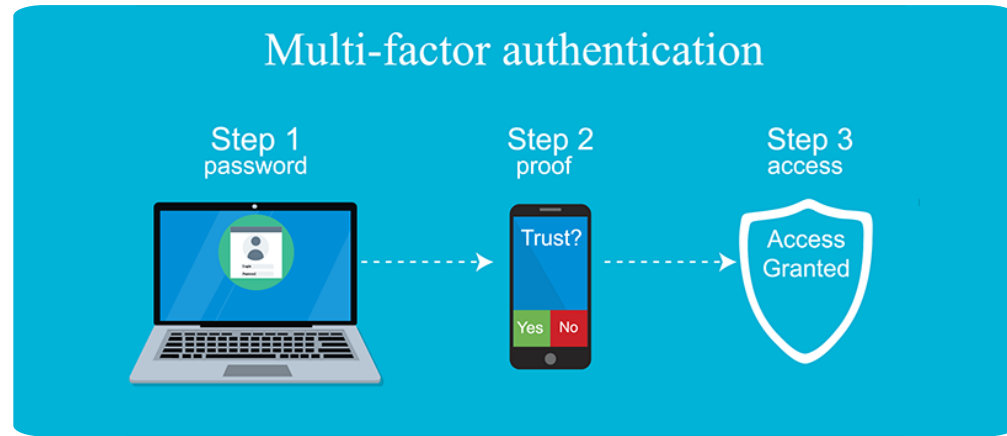
# Key Risks Identified

Severity ->	1 (Low)	2 (Medium)	3 (High)
3 (High Likelihood)	Low	High	Critical (Unauthorised Access, Phishing, Insider Threats, No Network Segmentation)
2 (Medium Likelihood)	Low	High	Critical (Lack of POLP, DNSSEC Attacks)
1 (Unlikely)	Low	Moderate	High

To prevent financial and reputational loss, critical risks should be addressed immediately!



**Solution:** Enforce MFA on all systems



**Cause:** Phishing & Lack of MFA

**Risk #1**




Unauthorised Access to  
Customer Data

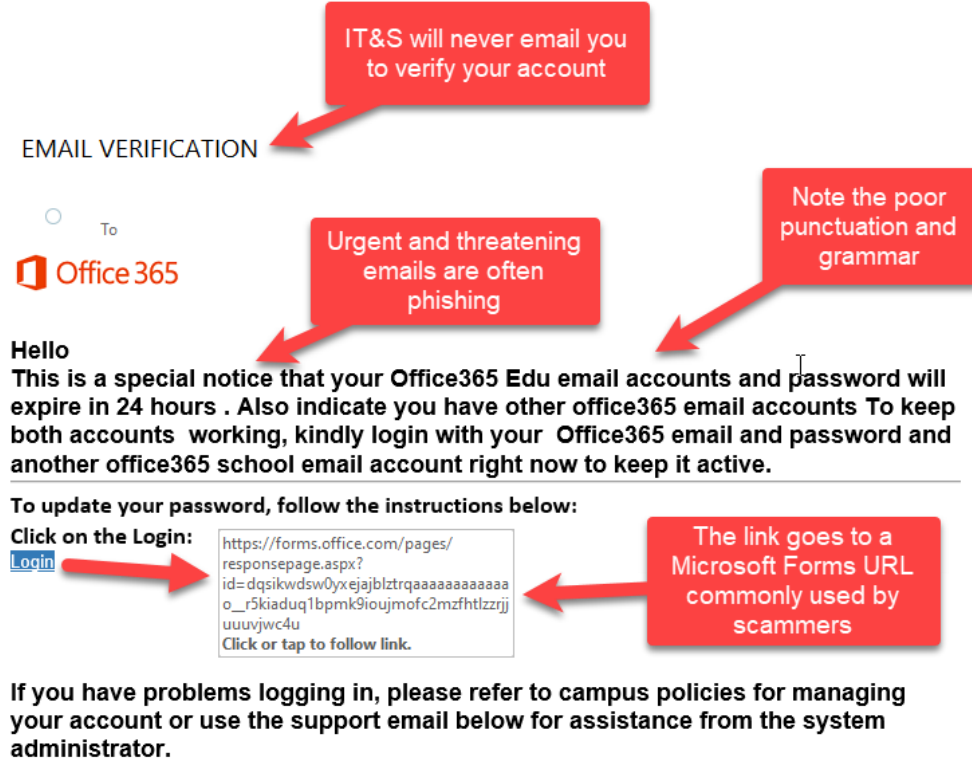


# Risk #2


## Social Engineering Attacks on Employees

**Cause -> Lack of cybersecurity training**

**Solution** -> Implement mandatory security awareness training 



<input type="checkbox"/>	<b>Password Policies</b>
<input type="checkbox"/>	Sniffing out Fraudulent Emails
<input type="checkbox"/>	Reporting Incidents
<input type="checkbox"/>	Secure Browsing Practices
<input type="checkbox"/>	Backing up Data
<input type="checkbox"/>	...



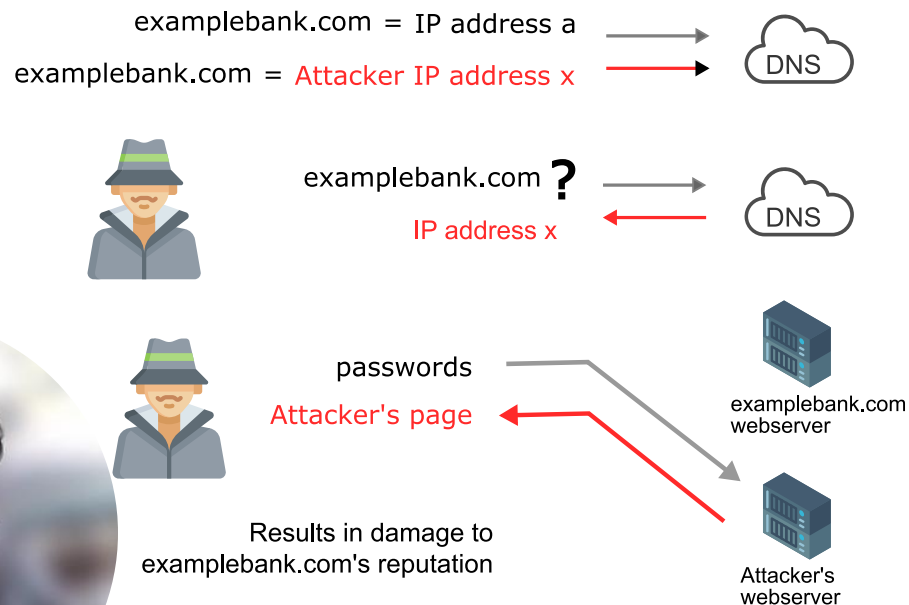
## Risk #3

### Fake Websites & Phishing Attacks

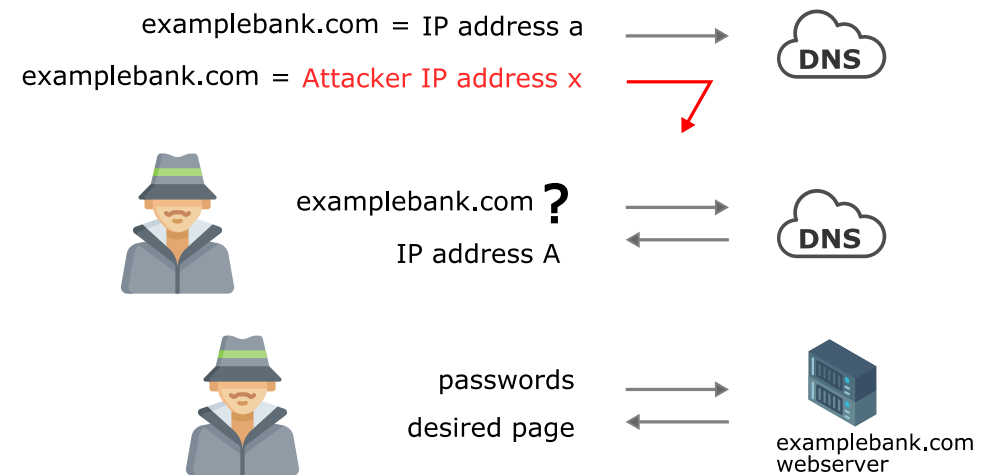
**Cause** -> Lack of DNSSEC

**Solution** -> Enable DNSSEC to prevent website impersonation

#### Without DNSSEC



#### With DNSSEC



## Risk #4

Overprivileged Employee Accounts

**Cause** -> No Principle of Least Privilege (POLP)

**Solution** -> Restrict access to only what's necessary ✓





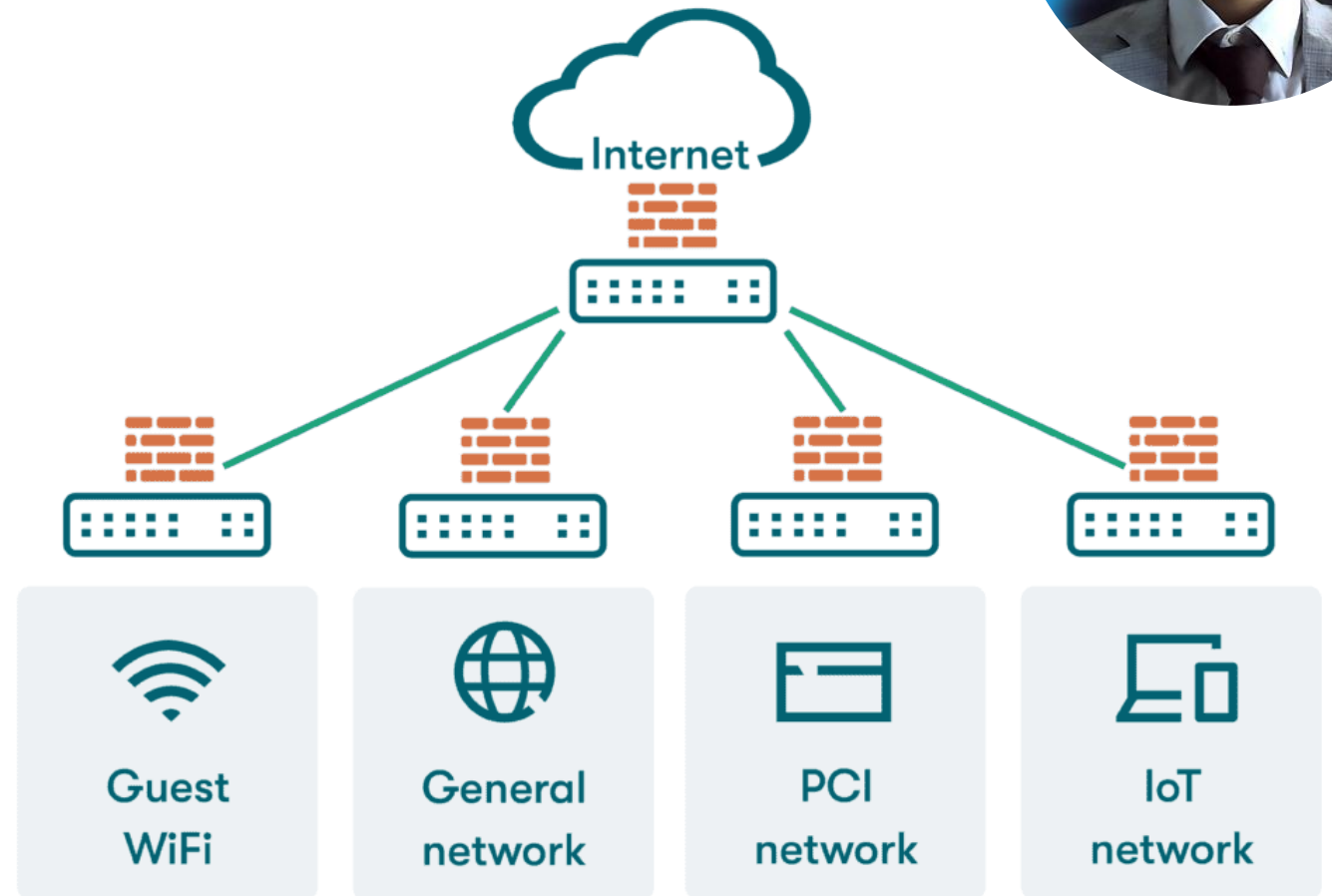
## Risk #5

Lateral Movement & Network Breaches

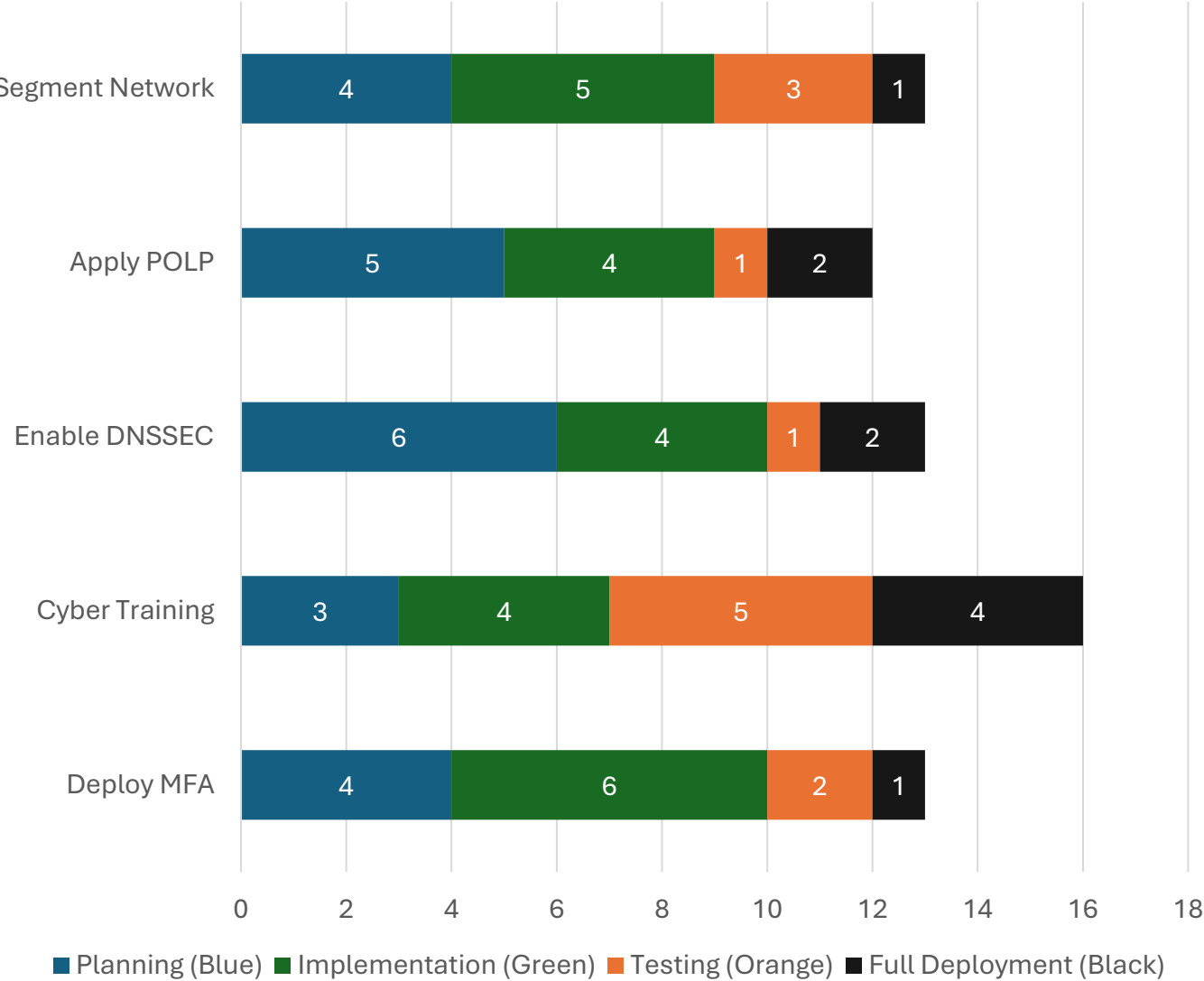
**Cause** -> No Network Segmentation

**Solution** -> Segment the network to contain breaches ✓

## Network segmentation



Implementation Timeline – Security Enhancements  
for Medibank (Weeks)



# Next Steps

- *MFA fully deployed by Q4 2025.*
- *Cybersecurity awareness program in effect by Q1 2026.*
- *Network segmentation & POLP finalised in early 2026.*





# Thank You

---

✉ Yasif Farook: [yasfarook937@gmail.com](mailto:yasfarook937@gmail.com)

**medibank**  
For Better Health