Risk Assessment

Organization: RetailNova Pty Ltd
Location: Melbourne, Australia
Industry: Retail (E-commerce & Physical Stores)
Prepared by: Cyber Security Professional
Date: Monday (Current Review)
Framework Used: NIST Cybersecurity Framework (CSF)

Client Overview

RetailNova Pty Ltd is a large retail organization with both physical and digital operations. Its technology environment includes a custom e-commerce platform, mobile application, cloud-connected POS systems, Salesforce CRM, SAP ERP, and AWS-hosted infrastructure. The organization processes and stores sensitive customer and employee data and relies heavily on third-party integrations for payments, logistics, marketing, and loyalty programs.

Given RetailNova's size, revenue, data volume, and history of cybersecurity incidents, the organization presents a high-value target for cybercriminals. Previous phishing incidents, ransomware attempts, and third-party data leaks indicate recurring exposure to cyber risk.

Key Assets

- Customer personal and loyalty data
- E-commerce website and mobile application
- POS systems across 85 stores
- SAP ERP and Salesforce CRM
- AWS-hosted infrastructure
- Employee credentials and remote access systems

Risk 1: Phishing and Credential Compromise

Risk Description:
Employees may fall victim to phishing attacks, resulting in stolen credentials and unauthorized access to cloud systems and sensitive data.

Likelihood: Likely
Impact: Major
Risk Level: High

NIST CSF Mapping:

- **Identify (ID.RA):** Risk of credential theft from prior incidents
- **Protect (PR.AC):** Weak authentication controls and reliance on passwords
- **Detect (DE.CM):** Limited ability to quickly detect compromised accounts

Key Mitigations:

- Enforce multi-factor authentication
- Improve email and phishing protections
- Strengthen ongoing security awareness training

Risk 2: Ransomware Disrupting Operations

Risk Description:
Ransomware could encrypt systems supporting stores, e-commerce, and backend operations, causing significant downtime and financial loss.

Likelihood: Possible
Impact: Extreme
Risk Level: High

NIST CSF Mapping:

- **Identify (ID.BE):** Critical dependence on digital systems
- **Protect (PR.IP):** Gaps in backup resilience and segmentation
- **Respond (RS.MI):** Need for faster containment and recovery
- **Recover (RC.RP):** Risk of prolonged service disruption

Key Mitigations:

- Implement offline and immutable backups
- Segment POS and corporate networks
- Conduct ransomware response testing

Risk 3: Third-Party Vendor Data Exposure

Risk Description:
Security weaknesses in third-party vendors may lead to indirect exposure of customer data, as seen in prior incidents.

Likelihood: Possible
Impact: Major
Risk Level: Medium–High

NIST CSF Mapping:

- **Identify (ID.SC):** Supply chain and vendor dependencies
- **Protect (PR.DS):** Over-sharing of customer data
- **Detect (DE.CM):** Limited visibility into vendor security incidents

Key Mitigations:

- Perform vendor security assessments

- Apply data minimization
- Strengthen contractual security and breach notification clauses

Overall Risk Posture

RetailNova faces a high cybersecurity risk profile due to its digital footprint, third-party integrations, and history of incidents. The most critical gaps align with NIST CSF Protect and Identify functions, particularly around access control, resilience, and supply chain risk.

Conclusion

To reduce risk, RetailNova should prioritize improvements in identity protection, ransomware resilience, and third-party risk management, aligned with the NIST Cybersecurity Framework. Strengthening these areas will significantly improve the organization's ability to prevent, detect, respond to, and recover from cyber incidents.