# Risk Management Strategy for Cheese Private Limited

(S4038096)

SaiTeja Bathula

RMIT University

Course Number: INTE1120 Introduction to Information Security

# ABSTRACT

Cheese! Pty Ltd. intends to start cheese sales at a second plant that will have more storage. They are thinking of how to set up their network and want to automate stock management. Two POS systems, two laptops, a database, and a web server for online purchasing are already in place at the company. Three new hires have been brought in to oversee the second site, only managers have access to private corporate records.

# Cheese Private Limited's Strategy for Risk Management

1) **What exactly is a cybersecurity plan, why is this company in need of one? What tools from Australia's 2020 Cybersecurity Strategy can this company use to be secure online?**

   A cybersecurity strategy is a detailed plan that describes how a company will defend its systems, data, and digital assets from online attacks. It entails locating weak points, preventative measures in place, and handling security crises. Cheese! Pty Ltd. needs a cybersecurity plan because they handle sensitive data, and they depend on networked devices to run their business.

   Cheese! Pty Ltd may improve its cybersecurity by leveraging the tools such as antivirus and cyber security awareness training provided by Australia's 2020 Cybersecurity Strategy, keeping abreast of risks and mitigation techniques, and partnering with industry and government partners to gain insightful information.

   **Resources:**

   The ACSC provides cybersecurity guidelines for company to enhance their cybersecurity posture. The 2020 Cybersecurity Strategy encourages cooperation and information exchange, enabling early threat identification and mitigation. The national strategy aims to secure 5G infrastructure, ensuring Cheese Pty Ltd's online activities and internet access security.

2) **What do risk management and assessment mean? Why would Cheese! Pty Ltd consider this to be a crucial business decision?**

   For businesses like Cheese! Pty Ltd to recognize possible risks and weaknesses like data breaches and cyber events, risk assessment is essential. Making educated judgments and creating plans to reduce these risks are both components of risk management. This is necessary for resource allocation, operational continuity, data

protection, and regulatory compliance. Cheese! Pty Ltd must manage finances, make investments in cybersecurity, and match security expenditures to their risk profile. If this isn't done, there may be legal repercussions and reputational harm to the business.

3) **What is the NIST framework, and how may Cheese! Pty Ltd utilize it to create a cybersecurity plan?**

   A methodical strategy for controlling and lowering cybersecurity risk is the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST). Identify, Protect, Detect, Respond, and Recover are its five main tasks. Cheese! Pty Ltd may create a cybersecurity plan using the framework. Assessing resources, risks, and vulnerabilities as well as seeing possible threats and putting preventative measures in place are all part of the "Identify" phase. The "Protect" function entails putting early threat detection methods in place and safeguarding systems, including web servers and laptops. Creating an incident reaction strategy and recovery techniques is the "Respond" function. Cheese! Pty Ltd can establish a complete cybersecurity plan with the use of this organized method.

4) **Provide a list of over five potential risks, vulnerabilities, and effects on the company to start a risk assessment. Utilizing a risk matrix, prioritize the risks.**

   Five cybersecurity threats, arranged in a risk matrix, are faced by Cheese! Pty Ltd. A data breach is of utmost importance because of its high probability and consequences. Malware outbreaks pose a serious risk because they can compromise critical data and cause operations to be disrupted. A critical risk that has a modest likelihood, but a high effect is insider threats. There is a medium chance of but a high effect from the loss of important firm records. Online sales disruption is less important yet has a medium chance.

| | High Likelihood | Medium Likelihood | Low Likelihood |
|---|---|---|---|
| High Impact | Data Breach | Inside Threats | - |
| Medium Impact | Malware | Loss of Data | Disruption of Services |
| Low Impact | - | - | - |

**5) Provide strategies and controls to transfer, reduce, or accept each risk.**

| Risks | Controls | Action |
|---|---|---|
| Data Breach | Encrypt Data<br>Back-up data | Mitigate |
| Malware | Anti-virus<br>Employee training for phishing emails. | Mitigate |
| Insider Threats | Implement user access control for least privilege access. | Mitigate. |
| Data Loss | Back-up Data. | Transfer |
| Disruption of Services | Implement standby systems. | Mitigate |

# References


- Australian Cyber Security Centre (ACSC) (2020) Australia's Cyber Security Strategy 2020, Australian Government Home affairs, 24th October 2023.

  https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

- World Economic Forum (WEF) (2020) Cyber Information Sharing Insight Report, World Economic Forum Website, 24th October 2023.

  https://www3.weforum.org/docs/WEF_Cyber_Information_Sharing_2020.pdf

- Cubic Nuvotronics (2022) National Strategy to Secure 5G, National Telecommunications and Information Administration, 24th October 2023.

  https://www.ntia.doc.gov/sites/default/files/publications/cubic-06252020_0.pdf

- Office of the Australian Information Commissioner (OAIC)(2023) Privacy, OAIC website, 25th October 2023.

  https://www.oaic.gov.au/privacy

- National Institute of Standard and Technology (NIST) (2023) NIST Cyber Security Framework, 25th October 2023.

  https://www.nist.gov/cyberframework