Cyber Sentinel Inc.

SECURITY MASTER PLAN

Prepared by:

Damon Duffy
34144772

Bhargav Raj Dutta
34834517

Klaryss Puno
35210149

Table of Contents

1.0 Executive Summary

This document is a Security Master Plan that provides a comprehensive framework for identifying and mitigating information security risks of Cyber Sentinel Inc., a medium sized software company supporting the oil and gas sector through specialized software development and seismic data processing. Given the highly critical nature of the organization's operations and client data, the company requires a proactive approach to secure its technical systems, physical infrastructure, human actors, and organizational procedures.

For each of the above-mentioned areas, relevant threats were identified, and their potential impacts are thorougly evaluated. The appropriate countermeasures are also developed and recommended which are guided by security best practices and aligned with the CIA triad of Confidentiality, Integrity, and Availability.

This document includes:

- A categorized inventory of organizational assets
- A threat-vulnerability assessment and risk ranking of resources
- Prioritized risk treatment strategies based on feasibility and criticality
- A tailored Cybersecurity Incident Response Plan (IRP) using industry templates
- Visual documentation including the company's floor plan and network infrastructure (*see Appendix A*)

2.0 Introduction

Cybersecurity has become a priority for organizations in an increasingly digital and interconnected landscape. Cyber Sentinel Inc., as a technology-focused enterprise, relies heavily on the integrity and availability of its information systems to deliver optimal services and maintain client trust. The development of this Security Master Plan document serves as a strategic blueprint for actively managing various threats that may compromise the confidentiality, integrity, or availability of the company's systems, data, and operations.

This document is completed on a series of investigative workshops that individually explored vulnerabilities in technical systems, physical infrastructure, personnel practices, organizational processes, and procedures. Each section identifies the key threats, evaluates their potential impacts, and recommends effective countermeasures within the boundaries of organizational resources. This master plan includes a risk management framework, asset inventory, and a tailored cybersecurity incident response plan.

2.1 Purpose and Scope

The purpose of this Security Master Plan is to guide Cyber Sentinel Inc. in safeguarding its critical information assets and business processes from different internal and external security threats. The plan aims to provide a proactive approach to identifying risks, evaluating their potential impact, and implementing the optimal risk-based controls across technical, physical, and human domains.

The scope of this document covers all relevant systems, infrastructure, personnel, and procedures associated with the current operations of Cyber Sentinel Inc. This includes internal staff, contracted personnel, and external visitors interacting with company resources. The plan also considers the organization's IT assets, network infrastructure, pre-existing policies, and incident response capabilities. It is intended for executive leadership, IT management, cybersecurity personnel, and stakeholders responsible for protecting the organization's digital environment and ensuring business resilience.

2.2 Company Overview and Organizational Structure

Cyber Sentinel Inc. is a mid-size software company specialising in developing software and hardware for the oil and gas industry, as well as providing services to oil and gas companies in processing seismic data to assist in locating new oil and gas fields.

Name : Cyber Sentinel Inc.

Address : Roxy Tower
: Guld Street Drive
: Perth 6000. Western Australia

Staffing : 500+ staff across various departments

Building : Basement - Carpark / Security Office / Loading & Unloading Bay
: Ground Level - Reception
: Level 1 - Building maintenance / Training room / R&D
: Level 2 - General Administration / Human Resource / Finance
: Level 3 - Sales / Software and technical support
: Level 4 - Information Technology / Server room
: Level 5 - Data Centre / Seismic Exploration
: Roof - Air-conditioner cooling towers, water tanks

Floor Plan : *See Appendix B*

Key Personnel : Ms. Klaryss Puno, Chief Executive Officer
: Mr. Damon Duffy, Chief Security Officer
: Mr. Bhargav Raj Dutta, Chief Information Technology Officer
: Ms. Klaryss Puno, Director Sales & Product
: Division Head - Research and Development
: Division Head - Software
: Division Head - Data Processing
: Division Head - Service and Technical Support
: Mr. Damon Duffy, Director - Back Office
: Manager Building and Maintenance
: Manager Officer Administration
: Manager Finance
: Manager Human Resource
: Manager Legal Department
: Mr. Bhargav Raj Dutta, Legal Officer

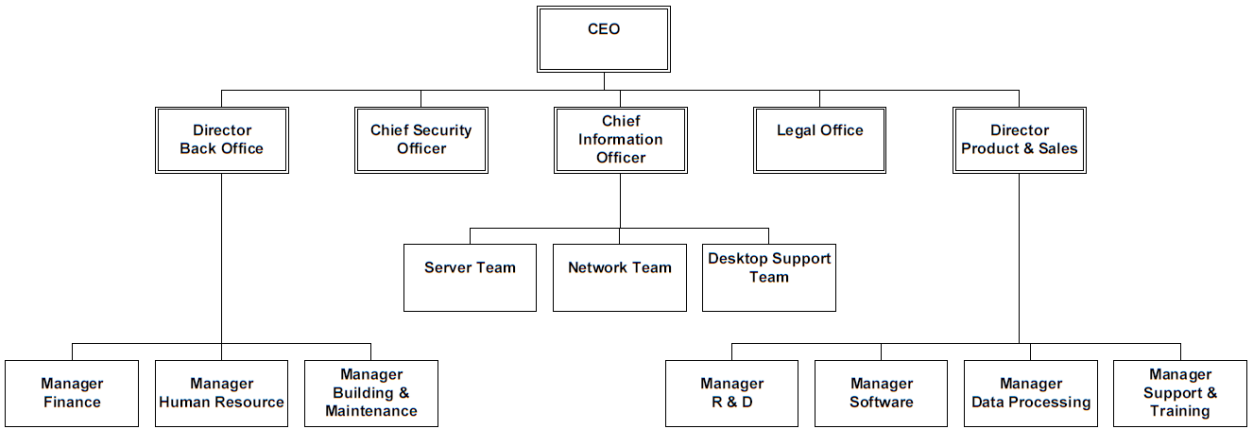


Figure 1: Cyber Sentinel Inc. Organization Chart

Establishing a clear vision of goals, influencing people, and bringing about long-term change, such as developing a security-conscious culture or aligning information security with business objectives, are all components of leadership. Management is more operational and focused on maintaining daily security controls, enforcing policies, and ensuring protocol compliance. Managers ensure efficient and consistent execution, while leaders set strategy and direction. Both are crucial: management deals with the "how," while leadership shapes the "why."

3.0 Understanding Information Security

According to NIST (National Institute of Standards and Technology), information security involves "*protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.*" On the other hand, computer security is the "*prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.*"

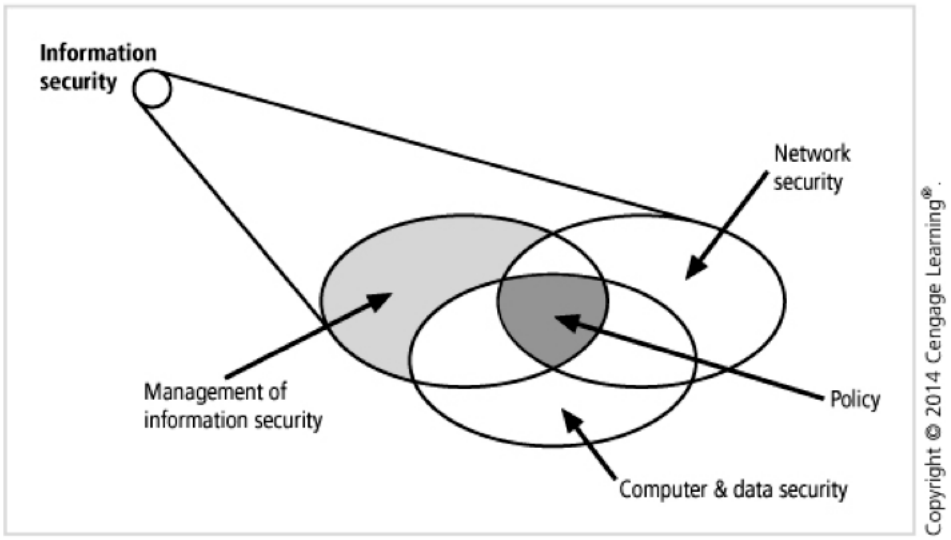


*Figure 2: Components of Information Security (*Whitman, M., & Mattord, H., 2014*)*

With these definitions at hand, the main difference between them is their scope, wherein infosec holds a more expansive reach extending to physical media, intellectual property, and other assets. The key elements of information security are as follows:

- Confidentiality – only authorized access is allowed
- Integrity – information remains accurate and unaltered
- Availability – information is accessible when needed by authorized users
- Privacy – data used only with the provider's consent
- Identification – the system recognizes individual users
- Authentication – verifies a user's identity
- Authorization – grants user access based on verified identity

The CIA triad includes Confidentiality, Integrity, and Availability. Altogether, these three principles guide the creation, development, and deployment of information security rules and policies to continually uphold the security status of an information system (Whitman & Mattord, 2018).

3.1 Components of Information Systems

An information system is an organized collection of resources designed to gather, process, store, and distribute information to help in the process of decision-making and control in an organization. These systems integrate several elements to manage data effectively and support organizational operations (Britannica, n.d.). The components of information systems are:

A. Hardware - physical devices such as PCs, servers, etc.
B. Software - These are the programs and apps that are used in an organization to perform tasks and process data
C. Data - This is a collection of information that an organization simplifies and analyzes to solve business problems
D. People - they are the subjects who interact with the system from all domains, such as IT, to non-technical

Some other components are processes and networks, which consist of procedures, policies, and laws followed by organizations. The network consists of devices connected in the IS and how they are communicating.

3.2 Information Security Management in the Organization

Information Security Management is an approach in an organization in which best practices are followed for protecting information assets and the information systems used by ensuring that the principle of CIA, i.e., Confidentiality, Integrity, and Availability, is maintained accordingly. The key characteristics of ISM are Confidentiality, which ensures that data can be accessed only by authorized persons; integrity, which ensures that the data is not altered and is accurate; and Availability, which ensures that data is available to authorized users. Some other characteristics are Privacy, Planning, Policy, Authorization, Authentication, and Protection.

3.3 Information Assets in the Organization

Information assets are essential in an organization to maintain business continuity and ensure smooth operations. The assets that need to be protected include Personally Identifiable Information (PII) of customers, financial and employee data, hardware such as servers and mobile devices, software including applications, operating systems, and custom tools, and networks (e.g., LANs, routers, firewalls) that facilitate communication within the organization. Additionally, the people who use the systems and the organization's reputation, including trust and credibility, are critical assets that need protection.

These assets must be protected to maintain business continuity, maintain the principle of Availability, and ensure that the organization complies with legal and industry best practices. Protection helps prevent any financial loss due to data breaches or cyberattacks, safeguards intellectual property, and helps maintain customer trust and organizational reputation in the industry. If these protections are not in place, it can lead to data breaches, legal penalties, operational disruption, financial losses, and damage to the organization's reputation.

Confidentiality, Integrity, and Availability are the foundation of protecting information assets. Confidentiality ensures that only authorized users have access to the data they require. For instance, a client's seismic data, or R&D source code, must be confidential to protect the data, and is done through controls such as:

- Encryption
- Access controls
- Multiple-factor authentication
- Data classification

Integrity ensures that the data is accurate, untampered, and trustworthy. Concerning the seismic data, for example, the reports generated from the data must not be altered to maintain the clients' accuracy. Information technology methods used to ensure this are:

- Checksum
- Version control
- Logging
- Secure patching

Availability ensures that the systems and data are accessible when needed and maintains the highest possible uptime. Systems used in the R&D and data processing units must be kept up, ideally 24/7, for continuous usage and monitoring. To achieve this, the following can be used:

- Raid systems
- UPS
- Backup internet
- Load balancing

3.4 Personnel Responsibility in Information Assets

A. InfoSec managers – lead protection efforts using PMBOK tools and methods
B. All employees share responsibility for following security policies
C. Communities of interest – including InfoSec community (protection), IT community (support), and general business community (policy and resources)

3.5 Key Areas of Security in the Organization

A. Physical security protects people, physical assets, and facilities from threats
B. Operations security ensures uninterrupted day-to-day activities
C. Communications security – secures all communication mediums and channels
D. Network security protects network devices, connections, and data

4.0 Resources at Risk

4.1 Technical Threats (Software and Systems)

A. Unpatched Virtual Machines and Operating Systems

The R&D business unit uses multiple operating systems for application development, including Windows 8.1, Windows 10 Pro, Server 2016, and Linux variants (e.g., Ubuntu, Red Hat Enterprise) and virtual machines (VMs). Due to their varying requirements and Software updates, inconsistent patching or outdated images can expose the current operating systems to remote code execution or privilege escalation attacks.

Upon successful attacks against the R&D information systems, the exposure of proprietary code or project files, such as distributed processing engines and remote monitoring tools, can be subject to intellectual property theft and potential data loss. The Office of the Australian Information Commissioner (n.d.) outlines the steps organizations must take under the Notifiable Data Breaches scheme involving the legal implications of this vulnerability observed in the Breach of the Australian Privacy Act 1988, specifically under the Notifiable Data Breaches (NDB) scheme, in the occurrence of any test systems containing identifiable client data. In addition, the threat results in possible non-compliance with ASD Essential Eight, particularly regarding patching applications and operating systems (Australian Signals Directorate, n.d.).

To counter the significant impact on the business and the development of critical projects, notable solutions must work hand in hand to ensure the overall integrity of the project and all involved information systems. Haletky (2009) explores the specific countermeasures to security challenges within virtualized infrastructures, including the placement of VM images in a safe and secure directory, solidifying the virtual hardware as well as the guest operating system, limiting access to the Backdoor of the virtual machine (in VMWare), and eliminating the presence of unknown virtual disks and VMs from the system environment. Essentially, the protection of virtual machines does not differ from the security practices employed on physical desktops, except for the treatment of strengthening the purely physical component and the strictly virtual component being done separately to ensure a higher level of security for both machines.

B. Data Interception During Remote Prototype Testing

In the beta field testing of the new real-time remote monitoring system, data is transmitted via satellite or landlines as part of the new project upgrades developed by the research and development business unit. Given the nature of the test operations, a threat against data in transit by attacker interception or tampering must be considered. Walters (2023) discusses the legal implications of unauthorized data interception resulting in the unauthorized collection, use, and storage of data. The following figure shows the data interception process where the author classifies processes that may be part of a shared interception and include, but are not limited to, key logging, intercepting data from a computer or network, packet sniffing, message reading and copying, programs and file copying, wiretapping, and eavesdropping.

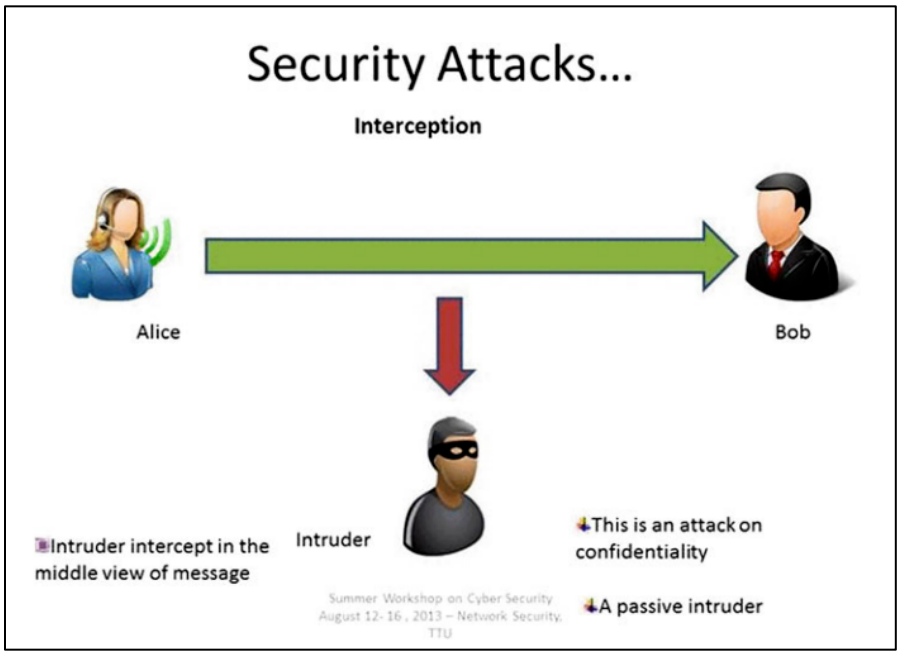


Figure 3: Data Interception Attack

Lindemulder and Kosinski (2024) further outlined that man-in-the-middle (MITM) attacks are a standard and sophisticated method of intercepting data, where attackers secretly relay and potentially alter communications between two parties who believe they are directly communicating. Such an attack might lead to privacy breaches due to the exposure of proprietary transmission protocol and financial implications an,d a reduction of competitive edge against market competitors. Common consequences include DNS poisoning, denial of service attacks, HTTPS sniffing with spoofed SSL certificates, and HTTPS sniffing with SSL stripping (Nath Nayak et al., 2010). Meanwhile, the legal implication of such a threat violates possible

legal obligations under the Australian Privacy Act and Telecommunications (Interception and Access) Act 1979, especially if test data is linked to identifiable clients or their infrastructure (Australian Government, n.d.).

The possible countermeasures against MITM threats involve compiling a comprehensive list of possible ARP poisoning and DNS poisoning, followed by the creation of a detailed table categorizing the types of poisoning attacks, their consequences, detection mechanisms, prevention techniques, and remedies—while considering existing limitations such as undesirable port blocking, packet restrictions, and limited activation of essential web services (Nath Nayak et al., 2010). In addition to these practices, Conti, Dragoni, and Lesyk (2016) emphasize robust countermeasures, including strong mutual authentication of communication endpoints, secure exchange of public keys, certificate pinning, and encryption to protect data integrity. Moreover, they recommend continuously monitoring the expected behavior of endpoints following the agreed protocol to detect anomalies.

This type of MITM attack underscores the importance of encryption, authentication protocols, and endpoint security to maintain the integrity and confidentiality of transmitted data during satellite or landline-based remote monitoring prototype testing, as emphasized by Lindemulder and Kosinski (2024).

C. General Denial-of-Service (DoS) Attacks Targeting Availability

A denial-of-service attack on the data processing servers could lead to disruptions when using the Shake and Quake Software to process and interpret seismic data for clients.

According to NCSC(2025), A denial of service (DoS) attack is an attempt to overload a website or network to degrade its performance or make it completely inaccessible. Typically, a successful DoS attack will result in the loss of availability of a part or all of a system and consume time and money to analyze, defend, and recover from it. Such an attack would disrupt the data processing being done for clients using the internally developed Software of Shake and Quake.

Such attacks have been carried out and have led to downtimes ranging anywhere from three days, such as in the case of the AWS DDoS attack in February 2020, up to six months, such as the case of the Google DDoS that occurred in 2020 (Nicholson, 2023). As per the (2025, April 9), the average cost of IT downtime is $5,600 per minute. However, it can vary based on how the business operates; regardless, such an attack would result in a heavy loss of money. The delays in the data processing may also breach the agreement with the customer, which could lead to legal ramifications.

In order to combat the threat of a Denial-of-Service attack, the data processing server can get DDoS protection services from a third party. Additionally, the servers should be monitored thoroughly to alert in cases where there is a spike in network traffic, potentially indicating a DoS attack.

D. Distributed Denial-of-Service (DDoS) Attacks

A DDoS attack is a cyber-attack in which multiple requests are sent to a target system, such as a website or a server, by using botnets. Those requests overload the server and are flooded with traffic, resulting in a crash, affecting availability, and making the site inaccessible to users. For example, in 2016, the Mirai botnet DDoS Attack was a massive attack performed on IoT devices that were not secure, and due to this, there was a disruption in internet services across the USA.

The impacts of this threat include:

- Downtime in services affects availability, which may lead to a loss of revenue and trust of the stakeholders
- There could be disruptions in operations if a server crashes, which could impact productivity
- The chances of data breaches increase if the attacker can perform more attacks after a DDoS.

The legal implications include:

- It could lead to not following the SLAs and data protection rules and regulations
- Stakeholders might sue the organization if it fails to maintain availability. (CISA, 2022)

The countermeasures against this threat are as follows:

- Confidentiality: By implementing WAF, using DMZ, and distributing the network in segments, we can isolate critical infrastructures.
- Integrity: It can be maintained by using IDS, IPS, and SIEM tools to monitor the network for any threats.
- Availability: Using DDoS mitigation services and ensuring the network's infrastructure is redundant to maintain availability.

E. Malware Infiltration via External Devices and Trojan Horse Programs

Malware introduced into the organization's information systems through external devices such as USB drives, external hard drives, or personal devices poses a risk to the business. The Support and Training business unit focuses on conducting onboarding, demonstrations, and training sessions. Throughout these sessions, a user can connect an external device to the computer while infected with malware. Such an attack happened to a credit union where a group of hackers dropped 20 USB sticks around the parking lot with malware. Fifteen of the USB sticks were found by employees and plugged into the system, where a malicious program ran and started communicating with the hacker's server (Lemos, 2016). These attacks can lead to data breaches or file corruption and must be considered.

Many methods to mitigate such attacks include running virtual machines instead of standalone computers for onboarding, demonstrations, and training sessions. Virtual Machines can allow for complete control over the devices and a layer of separation between the business network and the trainees. As the computers already have antivirus software installed and the firewall software is turned on by default, a review of the settings is necessary to ensure that malware detection and file quarantining are enabled. Finally, regular system backups would allow for a recovery in cases where a system is compromised and quickly recover with little system downtime.

To further protect the system, having security awareness training for the staff and new members would further assist in reducing threats from human error and enforcing positive cybersecurity habits.

As a specific kind of malicious software, a trojan horse disguises itself as legitimate to the user, and most of the time, users get Trojan malware by installing cracked versions of paid software. Once a Trojan horse is activated, it could gain root access, grant unauthorized access to threat actors, compromise individuals' confidential data, or add more malware to the system. An example is Zeus Trojan, a malware that was used to steal confidential banking data, and it infected more than 75000 accounts of prominent organizations, including NASA and Oracle.

The impacts of this threat include:

- Unauthorized access to confidential data could lead to data breaches and compromise.
- Financial Losses due to the compromise of confidential data
- Affects the principle of integrity and confidentiality.

The legal implications include:

- It will be a violation of data protection laws such as GDPR.
- Legal actions might be taken by the client side that is affected
- Regulatory fines and sanctions might be implemented for not following best practices in cybersecurity.

The countermeasures against this threat are as follows:

- Confidentiality: Implementing Access Control based on Role and Authenticating users.
- Integrity: Updating and patching the system regularly to fix any vulnerabilities
- Availability: Using antivirus software to detect and remove threats.

4.1.1 Summary of Software and Systems Threat Findings

Cyber Sentinel Inc.'s technical environment faces a diverse and evolving range of threats targeting its software, systems, and virtualized infrastructure. The threat assessment conducted across the organization reveals several critical vulnerabilities that, if left unaddressed, could result in significant data loss, operational disruption, reputational damage, and legal non-compliance.

- **Unpatched virtual machines and outdated operating systems** create security gaps, particularly in the R&D environment where a mix of platforms are used. These unpatched systems are susceptible to remote code execution, privilege escalation, and IP theft. Failure to maintain system updates may violate obligations under Australian Privacy Act 1988 and non-alignment with ASD Essential Eight guidelines.

- **Data interception during remote prototype testing**, especially over satellite or landline-based communications, poses a confidentiality risk to project transmissions. If data intercepted in transit includes client identifiers or proprietary protocols, the organization may be subject to penalties under the Privacy Act and the Telecommunications (Interception and Access) Act 1979. Effective encryption, endpoint authentication, and anomaly detection are essential to counter man-in-the-middle attacks.

- **Denial-of-Service (DoS) attacks**, both general and distributed (DDoS), threaten the availability of mission-critical services like Shake and Quake Software. These attacks can lead to processing delays, customer dissatisfaction, and breach of SLAs. DDoS events have shown high financial impacts in real-world cases and may result in legal claims from clients and stakeholders if availability is not maintained. A layered defense, including WAFs, SIEM systems, and traffic monitoring, is crucial to ensuring resilience.

- **Malware infiltration through external devices and Trojan horse programs** remains a high-risk vector—especially during training and onboarding sessions. USB-based malware can compromise business systems, as seen in documented cases of hardware-based attacks. Trojan horses disguised as legitimate software introduce the risk of credential theft, backdoors, and data exfiltration. Countermeasures must include endpoint protection, sandboxing using virtual machines, user training, and strict access policies.

In conclusioo, these threats emphasize the importance of continuous patching, secure communication, robust availability planning, and endpoint security. Ensuring the confidentiality, integrity, and availability (CIA) of systems demands a combination of technical controls, employee training, threat monitoring, and legal compliance frameworks. Strategic alignment with national standards such as the Australian Cyber Security Centre's Essential Eight will further strengthen the organization's defense posture and reduce systemic risk.

4.2 Physical Infrastructure Threats

A. Unmonitored Access to Critical IT Areas

The security assurance of any computer system decreases dramatically once an adversary has physical access to the components (McCreight, T., & Leece, D., 2016). Security assurance implies a strong focus on the physical security of entry points to, in this case, the servers and routers. However, as it currently stands, the company policy states that the server room and wiring rack are not locked during office hours to allow easy access to IT staff and locking them is left to the last person using them at the end of the day. Furthermore, with no security measures to log who enters and exits the server rooms and wiring racks, unauthorized individuals can attack through these points. Finally, with no surveillance system in place to monitor the server rooms and wiring racks, there is no means of monitoring the rooms to prevent a physical attack before it potentially occurs. This lack of security at such crucial entry points to the systems, paired with no obligation to escort visitors out, poses a serious threat to the physical security of the operations.

The impact of such an attack is highlighted by Karen Scarfone (NIST) et al. (2008): Servers host sensitive information, and many others, such as public-facing Web servers, should be treated as sensitive because of the damage to the organization's reputation that could occur if the servers' integrity is compromised. Furthermore, if an unauthorized individual were to exploit the weak entry controls on the wiring rack, they could gain direct access to the network, allowing them to install malicious devices to infiltrate. Finally, there is a risk of physical damage or theft to the servers and router.

As another aspect of physical security, tailgating is a serious concern. It describes a security breach where an unauthorized person closely follows an authorized individual through a secured access point, such as one protected by electronic identification cards (PR Newswire, 2006). Given that the company employs various contractors and vendors on their current operations where there is no escort enforced during exit, and passenger lifts operate 24/7 with unlocked stairwells, an opportunity for unauthorized individuals to tailgate staff or contractors which can result in gaining physical access to sensitive business units such as IT, R&D, and Data Processing through tailgating.

Lasky (2022) categorizes tailgating breaches into three types based on the intruder's intent: malicious intrusion, where unauthorized access is deliberate and aimed at causing harm; negligent intrusion, where access is intentional but without harmful intent; and accidental intrusion, which happens unintentionally and without any motive to cause damage. The author investigates the impacts of tailgating through insights from renowned industry leaders. The effects of tailgating, as discussed, pose significant risks by enabling unauthorized individuals to bypass physical security controls, potentially compromising valuable organizational assets and causing severe disruptions to business operations. An example presented in this study is Sony's case, where a single unauthorized physical access event led to a massive organizational breach. This demonstrates that even robust cybersecurity defenses are ineffective if the physical entry and security aspects are not appropriately controlled. In addition to this, it has been found that physical security measures often lag behind digital protection practices, which leaves organizations exposed to insider threats and social engineering attacks that exploit access-controlled physical entry points.

In terms of possible legal implications of the threat, this may violate the Australian Privacy Act 1988 in the case where tailgating results in a notifiable data breach. Moreover, failure to monitor physical access control caused by tailgating may breach principles as stated in the Protective Security Policy Framework (PSPF), specifically when handling classified information or critical business assets (Australian Government, n.d.).

As a countermeasure against tailgating threats, Lasky (2022) recommends the implementation of three key countermeasures. Firstly, the organization should adopt next-generation, intelligent Physical Access Control Systems (PACS) with the capability of integrating analytics and real-time decision-making to detect and prevent unauthorized entry. Secondly, intelligent turnstiles or speed gates deployed in high-traffic locations such as building lobbies create a physical barrier that gives one credential access to only one individual. This is primarily intended for contractors and vendors working mainly after office hours and unescorted visitors entering the

company premises. Thirdly, deploying tailgate detection devices on critical entrance points can add an essential layer of automated security that sends out automatic alerts to the rightful security personnel when several people attempt to enter using a single authentication event.

Meanwhile, as a general measure, the ANSI/BICSI Best Practices paper (2011) recommends providing a server room-secured video monitoring and access control system database (Lensu, V., 2013). Video monitoring of the server would allow constant monitoring of the entry point. With surveillance cameras with alert functionality, any movement in the server could be alerted to and monitored. Additionally, electronic locks can be installed on doors requiring badge access to open and log activity. Finally, a renewed policy that ensures that visitors are escorted in and out of the premises, with sign-ins and out, will ensure that no unauthorized persons can maliciously or unintentionally get through security entry points, reducing the risk of such an attack.

In addition, PR Newswire (2006) suggests that the organization can employ high-frequency RFID (Radio Frequency IDentification) badges or smart cards in combination with biometric facial recognition that matches the cardholder's face for the authorized personnel to open doors and enter secure zones. This kind of integrated system uses facial recognition technology to strengthen its security by ensuring the person holding the ID badge is its rightful owner. In the case of a mismatch between the badge and the individual's face, security staff are notified accordingly to respond to the failed attempt and execute further organizational security protocols. Finally, Ritchey (2019) highlights the importance of awareness programs and employee education that can be employed to fortify the culture of security within the organization.

B. Power Outages in Critical IT Infrastructure

The business processes rely heavily on server-based data processing, client services such as the seismic data processing through Shake and Quake, and internal operations such as the R&D projects that are ongoing, and the servers make use of Symantec Backup Exec software to back up the servers onto an HP 1/8 G2 Tape Autoloader. Suppose the power were to go out due to natural disasters, lose of power in the city’s grid, or even a malicious power attack. In that case, a power attack is a malicious workload that can generate power spikes on multiple servers simultaneously, which could lead to undesired power outages. (Xu, Wang, Xu, & Wang, 2014). In this instance, it could be through malicious client data being sent for processing.

The impact of a power outage on the organization could lead to significant complications. The R&D projects that are time-dependent in gaining market share could be delayed through a power outage or corrupted as a result. The project delay could lead to a loss of market share, costing the company upwards of 10% (around $100 million). Services such as seismic data processing through internal software, Shake and Quake, would also be delayed and potentially corrupted. This could lead to legal complications with the service agreement between the organization and the client, leading to further financial and reputation loss.

An example of a power outage and its effects could be Cloudflare's power outage in 2023, where a critical facility lost power for an extended period, caused by power grid maintenance (Matthew P., 2023), which was out of their control. However, it still led to customers complaining and a loss of trust. If they had backup generators available, then it is possible that the servers could have been online throughout grid maintenance.

In order to mitigate such a risk, the company could make use of a backup generator or an uninterruptible power supply (UPS); Uninterruptible power supply (UPS) system provides clean, conditioned, and uninterruptible power to the sensitive loads (Aamir, Kalwar, & Mekhilef, 2016), which means that if the servers are equipped with UPS, then they would be allowed adequate time to shut down properly avoiding corruption and data loss. A backup generator for the whole building would enable all systems to utilize such a service; however, it would cost much more to maintain.

C. Thermal Risks and Overheating in Equipment Rooms

The deployment of new research and development projects entails a high level of dependency on the company's physical infrastructure to execute the expanding demands of each project. Zeng et al. (2021) highlight that data centers, including wiring closets, server rooms, and data processing rooms, contain a high concentration of valuable electronic equipment. Because of this, any disruption to their operation can have serious consequences, necessitating stricter loss prevention strategies. From a risk assessment perspective, threats like fire, smoke, corrosion, and water damage must be carefully considered. In addition, thermal hazards such as overheating can result in significant risks, particularly in areas like wiring closets that lack air-conditioning and in server and data processing rooms where cooling systems may represent a single point of failure.
According to Wang et al. (2013), elevated temperatures within data centers can drastically reduce the lifespan of servers, as electronic components tend to degrade more rapidly at higher operating temperatures. Furthermore, excessive heat

increases the risk of thermal emergencies, which may trigger system shutdowns and compromise the availability of IT services. A real-world example occurred on the 5th of July 2010, when Wikipedia experienced downtime due to a cooling unit failure that caused server overheating, ultimately leading to a data center power outage. This incident highlights the importance of accurate heat detection and strategic airflow management to prevent disastrous outages from happening.

In terms of possible legal implications of the threat, this violates possible legal obligations of the Australian Privacy Act 1988, specifically under the Notifiable Data Breaches scheme, where the overheating incident leads to a system crash or loss of data involving sensitive client information. In addition, any failure to maintain safe operational working environments is also a possible breach of employer duties under the Work Health and Safety Act 2011 (Australian Government, n.d.).

As a countermeasure against overheating threats in these critical IT infrastructure areas, namely wiring closets, server rooms, and data processing, it is ideal to adopt intelligent thermal management strategies. Traditional thermal monitoring methods, such as wired probes and thermostats, only offer a limited resolution, which is insufficient for detecting certain areas with high temperatures ("hot spots") and eventually enabling energy-efficient cooling. As an advanced solution to this, wireless sensor networks (WSNs) can be used as they provide more detailed and real-time temperature data as well as broad spatial coverage to monitor affected areas (Wang et al., 2013).

Moreover, the most straightforward approach is a practical airflow and cooling design. As server power increases, the cooling demand for these systems increases accordingly, significantly impacting these infrastructures' overall energy consumption. Poor air distribution caused by inefficient placement of wiring closets and CRAC (Computer Room Air Conditioning) units can lead to hot air recirculation and cold air bypass. (Nada, Said, & Rady, 2016). Due to these, aisle containment strategies must be implemented, optimizing CRAC layouts and regularly assessing airflow paths to ensure efficient cooling performance and overall protection of the company’s physical infrastructure assets.

D. Theft or Loss of Physical IT Equipment

Physical theft is the unwanted or unauthorized stealing or removal of an organization's devices, such as PCs, laptops, servers, hard drives, or sensitive data or PII. This threat is dangerous as this equipment might have unencrypted and easily accessible data.

The theft of IT equipment due to a lack of physical security, such as a lack of monitoring by guards, inadequately secured environments, and poor protection of data centers, can lead to these thefts. For a real-life example, 2006, a laptop was stolen, and an external hard drive was compromised at the Department of Veterans Affairs in the USA, which comprised data of 26.5 million veterans. A lot of sensitive data was leaked. (*EPIC - Spotlight on Surveillance - May 2006*, n.d.)
It can lead to loss of sensitive data, harm to critical physical infrastructure, disruption in operation, downtime, and loss of trust by stakeholders. Legal implications could be that the organization may face legal actions under the Privacy Act 1988 (Australia), and legal impacts will differ from country to country. It can also lead to financial penalties due to a lack of responsibility, lawsuits, and investigations. (Oaic, 2024)

To maintain Confidentiality, the data should be encrypted even when it is at rest on portable devices such as laptops and phones. Integrity can be maintained by implementing strict RBAC and keeping logs of system usage, IP address, and location. Moreover, availability can be maintained by keeping all the data in the cloud backed up and using redundant systems to avoid dependency on a single system. However, for risk management CCTV surveillance, only biometric authorized access for server rooms or places where critical assets are located can be added, and security awareness training for the employees could also be provided.

E. Rogue Access Points and Unauthorized Network Devices

One of the physical threats is the installation of Rogue access points in an organization in which these APs could be physical devices such as laptops, smartphones, or IoT devices; sometimes, it could be software, wireless devices, and applications as well that are being installed without the consent or awareness of the Network Administrator of the Organization. These devices could be connected maliciously by threat actors or accidentally by employees, which will help the bad actor intrude and compromise the system (Libeer, 2024).

These APs also work by exploiting the network infrastructure in which threat actors use common devices, such as having a personal wireless router or USB-based WIFI dongle. When it's plugged into the organization's network, it creates a backdoor for the threat actor. Once an intruder gains access to the network, it's easy for him to perform a MITM (man-in-the-middle attack), eavesdrop on the network traffic, inject malicious code into the network, and crash it. For a real-life example, in 2005, a company named TJX had a data breach in which threat actors exploited a less secure wireless network using Rogue access points across their outlets, and it led to a massive data breach of more than 94 million credit and debit cards (Marvin, 2023)

Rogue APS impacts could be data breaches, compromise of system access, system and network downtime, unauthorized access to internal data, compromise of PII of customers, and many more impacts. Legal impacts could be that organizations might have to pay hefty fines if they are unable to detect and remove these devices as they don't follow GDPR rules accordingly. Moreover, there will be damage to reputation, and the clients could sue them due to the compromise of their data (Twingate, 2024).

To maintain the principle of Confidentiality, organizations can deploy a Wireless Intrusion Prevention System (WIPS) that will help monitor any intrusion wirelessly and prevent unauthorized transmission (Scarfone & Mell, 2007). For the principle of integrity, audits of the connected devices and managing a record of the devices are helpful. Availability can be achieved by maintaining the policy of banning the connection of personal devices to the network and training staff on unauthorized access. Regarding Risk Management, using a ZTA (Zero Trust Architecture) and testing wireless devices can reduce the risk of intrusion (Twingate, 2024).

4.2.1 Summary of Physical Infrastructure Threat Findings

The analysis of physical infrastructure threats at Cyber Sentinel Inc. reveals a range of critical weaknesses that, if left unaddressed, could jeopardize system availability, compromise data confidentiality, and disrupt business continuity. The key conclusions from the workshop are outlined below:

- **Unmonitored access** to server rooms and wiring closets creates opportunities for unauthorized entry, potentially leading to data breaches. The lack of surveillance and strict visitor escort policies highlights the need for role-based physical access control and continuous monitoring mechanisms.

- **Tailgating** remains a physical security gap due to unguarded entry points and unescorted vendor access. This requires enforcement of stricter access controls such as biometric systems, turnstiles, and continuous physical access awareness training.

- **Power outages** present a major threat to data processing operations, particularly in the absence of backup power systems. Investing in uninterruptible power supplies (UPS) and generator systems is essential to preserve system uptime and protect data integrity during critical project activities.

- **Thermal hazards** in areas like wiring closets and server rooms pose risks of equipment failure and data corruption. Enhanced cooling strategies, structural safeguards, and intelligent thermal monitoring can mitigate this threat and support operational stability.

- **Theft of IT equipment**, especially devices containing unencrypted data, introduces legal and operational risks. Mitigation should include encrypted storage, cloud-based redundancy, RBAC policies, and physical protections like CCTV, access badges, and biometric locks.

- **Rogue access points** represent a hybrid threat—rooted in both physical and network vulnerabilities. WIPS (Wireless Intrusion Prevention Systems), Zero Trust Architecture (ZTA), and regular device audits are essential to detect and eliminate unauthorized wireless connections that could expose internal systems to external compromise.

Together, these findings reinforce the need for layered physical security, clear procedural enforcement, and continuous monitoring to align with the principles of confidentiality, integrity, and availability (CIA) and ensure the resilience of Cyber Sentinel Inc.'s physical infrastructure.

4.3 Human-Centric Threats

A. Insider Threats and Privileged Misuse by Employees

The R&D team is currently working on a major project to optimize the existing custom-designed chip or software. Developments on this project involve deep access to code repositories and testing environments, which are accessible to trusted personnel (i.e., research and development staff members) that may use their privileged access for their personal purpose and motivation namely, fraud, theft of Intellectual Property (IP), and sabotage of the existing business infrastructure (Nurse et al., 2014). Without strong controls in the R&D business unit, a staff member can maliciously copy sensitive files (e.g., beta software or custom chip specs) to external media or leak said information to market competitors.

These threats and privilege escalations are malicious actions by users authorized to use the system with legitimate access. The system's stakeholders, such as employees, business partners, etc., can be an insider threat to an organization and may misuse their privileges to compromise data or perform external attacks. These threat actors' actions lead to the creation of vulnerabilities and privilege escalation.

In 2019, there was a data breach in which a threat actor who was a former employee at AWS exploited Capital One's cloud, misconfigured a firewall, and gained access to over 100 million records of customers, where PII was compromised (Capital One, 2019).

Insider threats represent one of the most difficult challenges to detect and prevent within an organization, as internal staff hold varying levels of access to critical information systems that can be exploited for malicious purposes. Whitty et al. (2024) found that insiders have access to organizations' sensitive data, systems, and business secrets to steal these information assets for their financial gain and reputational damage to the business. Moreover, the impact of such a threat poses a unique challenge to the overall security of the project, as insiders can extend the malicious act over a long period (Björkman et al., 2022). The legal implications of said threat result in possible IP theft prosecution under the Australian Copyright Act 1968 as stated in the Copyright Act 1968 (Australian Government, 1968) and the risk of data breaches under the Australian Privacy Act if any client or partner data is involved in test environments as outlined by the OAIC (n.d.). Moreover, legal implications as per Australian laws could be the Cybercrime Act 2001 (University of New England. (n.d.), which addresses unauthorized access, organizations may face fines.

Wisnubroto et al. (2023) emphasized that a combination of technical and non-technical measures is required to address the insider threat in an organization. Namely, Nurse et al. (2014) propose a variety of these approaches to mitigate the risk of insider attacks, focusing on prevention, detection, and response, which includes countermeasures such as managing negative issues in the workplace, considering threats from insiders and business partners in business-wide risk assessments, logging and auditing employee's online activities, and creating a structured insider incident-response plan. In addition, fostering a strong security culture in the research and development business unit by training employees and external contractors on insider threats can strengthen the security of sensitive and developing business assets (Wisnubroto et al., 2023).

Furthermore, countermeasures to maintain confidentiality include implementing role-based access controls and applying the principle of least privilege so users can do their work as assigned. In terms of integrity, deploy the DLP systems to monitor any anomalies, and the user's behavior can be analyzed from logs and their activities, which can be done by a SIEM tool as well. For availability, training all the employees, and performing a background check on the department staff members.

B. Poor Cyber Hygiene Practices Across Departments

Poor cyber hygiene continues to pose a significant risk to organizational security, especially when practiced by internal staff with elevated access to critical systems and sensitive data. As Vishwanath et al. (2020) explain, cyber hygiene refers to routine digital practices and behaviors that maintain an organization's security health. Drawing from public health principles, the European Union Agency for Network and Information Security (ENISA) emphasizes that cyber hygiene should be treated like personal hygiene, where daily habits and periodic check-ups ensure digital systems remain secure and resilient.

An example of poor cyber hygiene is reusing the same passwords across multiple applications that store identical or sensitive data. As highlighted by VMware, this practice can significantly increase the risk of financial fraud and data compromise for consumers, banks, and financial institutions ("Poor Cyber Hygiene Puts Consumers and FSIs at Greater Risk of Fraud," 2018). The legal implications of said threat, such as weak password practices, failure to use multi-factor authentication, or improper handling of credentials, may potentially lead to unauthorized access and data breaches. Under the Australian Privacy Act 1988, organizations must take reasonable steps to protect personal information from misuse, interference, and unauthorized access. Failure to do so may trigger obligations under the Notifiable Data Breaches (NDB) scheme, requiring notification to affected individuals and the Office of the Australian Information Commissioner (OAIC). In negligence cases by directors, there may also be implications under the Corporations Act 2001, particularly regarding directors' duties to manage foreseeable cybersecurity risks (Australian Government, n.d.).

In risk management against poor cyber hygiene among employees, adopting stronger cyber hygiene practices is a proactive strategy for minimizing the likelihood of cyber threats. As Salem and Sobaih (2023) explain, cyber hygiene consists of simple daily routines such as strong password management, recognizing phishing attempts, and secure reporting protocols, all of which contribute to maintaining a secure digital environment. Clinton (2022) emphasizes that while technical defenses are essential, cybersecurity must be a shared responsibility across the entire organization, forming the base of any competent security program.

Effective implementation also requires continuous user education. Kamerer and McDermott (2023) argue that all employees, not just IT staff, must understand and apply cyber hygiene practices. This does not demand advanced technical knowledge but does require regular training and reinforcement of best practices, particularly before users are given access to critical systems. Ensuring staff across departments receive ongoing cyber hygiene education helps cultivate a security-aware culture and supports long-term risk mitigation.

C. Social Engineering and Phishing Exploits

Internal staff, particularly those in managerial or administrative roles, are prime targets for social engineering attacks such as phishing, where attackers exploit routine communication channels to deceive employees into revealing sensitive information. In other instances, attackers execute malicious actions that compromise the organization's information systems. Kerr, Gammack, and Boddington (2011) explain the concept of social engineering as an activity where a criminal gains an employee's trust over a period of time as part of a personal motivation to abuse it eventually. In addition to these are fraudulent activities, including spoof websites or emails, or phishing and pharming, where official-looking yet fraudulent emails request sensitive information such as passwords or bank account numbers. Sarpong Adu-Manu, Ahiable, Appati, and Mensah (2022) review the following example as a common type of phishing email where the attacker attempts to imitate an official email from Microsoft directed to an unsuspecting employee from the Internal Staff category:

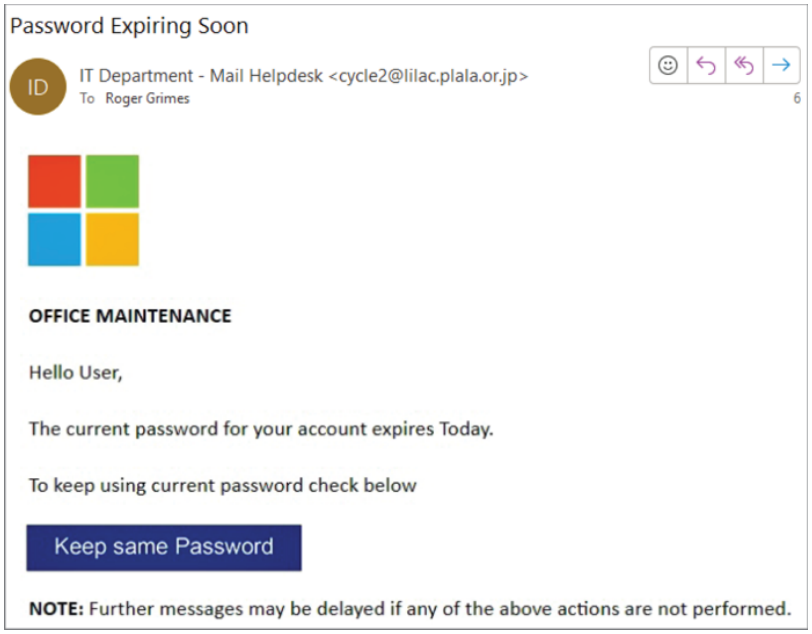


Figure 4: Example of Phishing Attack

The possible impacts of successful phishing attacks can cause significant financial loss for an organization or even an individual. Furthermore, it may also result in sensitive organizational information being possessed by malicious owners. In extreme cases, attackers seize complete control and refuse the organization's services, otherwise known as Denial of Service (Kerr, Gammack, & Boddington, 2011). Meanwhile, the legal implications of such a threat violate possible legal obligations under the Australian Privacy Act 1988, particularly under the Notifiable

Data Breaches (NDB) scheme, if unauthorized access to personal or sensitive client information occurs. Organizations may also breach governance expectations outlined in the Corporations Act 2001 if it is found that directors or officers failed to implement reasonable cybersecurity measures to prevent foreseeable social engineering attacks (Australian Government, n.d.).

From a risk management perspective, social engineering threats such as phishing can be addressed using a structured approach involving risk identification, assessment, treatment, and monitoring. The organization must identify phishing as a credible threat and assess its likelihood and impact through a risk matrix. Following this, treatment strategies to enforce cybersecurity awareness programs for risk mitigation, such as conducting phishing simulations and deploying globally used anti-phishing standards for email verification, Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF), and Domain Keys Identified Mail (DKIM), can be implemented. These measures aim to reduce the likelihood of successful attacks and their potential damage, particularly with email verification technologies, which ensure that a specific sender domain is genuinely from the domain it identifies with (Grimes, 2024). Additionally, the risk management cycle should continuously monitor phishing trends and response effectiveness, ensuring that defensive mechanisms remain adaptive and updated with evolving attack methods. Apart from this approach, the organization must focus on employees' education in reporting, mitigating, and recognizing phishing and social engineering attempts. This can be done through periodical training in phishing test simulations.

D. System Misconfigurations by Internal Users

IT support staff may unintentionally misconfigure critical IT systems such as firewalls, backup schedules, or access permissions, leading to security gaps in the environment or service disruptions through errors. Furthermore, misconfiguration of network access controls can leave the organization vulnerable to malicious virtual attacks.

IT support staff are generally tasked with setting up new devices for new staff members. Currently, the company ensures that the client computers have the same antivirus software installed and that the operating system’s firewall is turned on. When configuring the computers and devices, with a wide range of access controls to set up the devices, staff may overlook three common misconfigurations, namely, shadowing, correlation, and redundancy (Alicea & Alsmadi, 2021); shadowing occurs when two rules with similar scopes are included in the firewall list, leading to the rule with a more narrow scope never activating, correlation is when two rules capture the

duplicate packets but need to execute specific actions. Redundancy occurs when two rules capture and execute an action on the duplicate packets (Alicea & Alsmadi, 2021). These three misconfigurations can leave gaps in the security for exploitation. Additionally, suppose the support staff unintentionally opens unneeded ports. In that case, the devices may also be susceptible to a port scan attack.

An example of an attack on a misconfigured system would be the data breach at Equifax in 2017. The data breach occurred as, amongst several vulnerabilities, the attackers found a gap in the firewall that allowed them to send malicious code through the system to be executed on the servers. This attack led to Equifax $1.38 billion of lawsuits, settlements, and significant loss of trust (Breachsense, 2024).

Such vulnerabilities can lead to attacks, as aforementioned, resulting in the loss of the systems and business downtime, potential loss of data, and a breach of confidentiality. Suppose these vulnerabilities were exploited similarly to Equifax, leading to a data breach. In that case, there may be legal implications for breaching the Privacy Act 1988, which could lead to further legal ramifications.

In order to mitigate these issues, it is best to ensure that support staff use stateful rules when considering the firewall, as stateless rules are more prone to misconfigurations (Deng et al., n.d.). Risk management can mitigate the threat through regular firewall and system audits and configuration monitoring to ensure that all appropriate steps are taken. The risk can also be avoided using a policy-based automation tool to ensure the systems are automatically set to follow the defined rules.

E. Delayed or Inconsistent Security Patch Management

The threat of delayed security patch management can be caused by IT support staff neglecting to patch or update client PCs or servers. Patches not being applied are especially problematic, as the current setup on client PCS and all servers has automatic software patching disabled, and the policy states that new patches are only applied once compatibility has been ensured.

Software security patch management refers to applying patches to the security vulnerabilities in the software products and systems deployed in an organization's IT environment (Dissanayake et al., 2021). Despite the importance of such patches, support teams may delay or neglect pushing new patches or updates on devices and servers due to time constraints, such as the current two projects the company is working on, or the system's complexity. Staff not applying patches can leave the systems vulnerable to known exploits.

An example of such an attack is the attack on Equifax. As aforementioned, the attack occurred in 2017 and led to a leak of over 140 million Americans' private data (Dietrich et al., 2018); while the gap in the firewall allowed for the attacks to send malicious code to the server, another Apache-related vulnerability was well known and was used to enable the maliciously sent code to gain access to the database. Ultimately, the staff could have prevented the attack as a patch had been made for the said exploit; however, it was never applied to the systems by the IT staff.

The potential lack of security patch management can impact the systems and the company. If patches are not applied, once compatibility has been ensured, then attacks can exploit the known vulnerabilities, potentially leading to data loss, compromised systems, or malware injected into the system. Once again, if a data breach were to occur, then under the Privacy Act 1988, the company may be subjected to fines. Additionally, if an attack happened due to not applying a security patch, then a downtime in the system would lead to delays in the two projects currently underway.

In order to mitigate such an attack, the company has multiple methods to pick from: ensuring everything is backed up, documenting network infrastructure, documenting the unique software on the devices and systems, implementing change control processes, or performing risk assessments on the patches. (Lanz, 2024). IT support staff can apply risk management by mitigating the risk through routine update schedules, using the patch testing environment server to test compatibility, and enforcing a higher security standard. Cybersecurity insurance, such as Equifax's case, can also partially transfer the risk.

F. Credential Misuse by Third-Party Contractors

In an organization, a significant threat that is mostly ignored and not taken seriously is that third-party vendors and contracted personnel can misuse or compromise their login data through either phishing, negligence, or malware infection. As these contractors access the system through their temporary accounts, these credentials can be a vulnerability for the organization. If these are not handled properly, this could also lead to zero-day exploits and an increase in the organization's attack surface.

A real-life example is the Target Breach in 2013, in which threat actors/hackers stole network credentials from a contractor and used this access to attack the network infrastructure. Later, it led to a data breach in which 40 million credit card data were compromised (Krebs, 2014).

The impacts can be dangerous, such as data theft, downtime in service, and damage to reputation, and legal actions could be taken under the Australian Legislation. Specifically, the Privacy Act 1988 will be applied, which suggests organizations report any data breaches related to PII (Personal Identifiable Information).

In order to mitigate risks and maintain the principle of confidentiality and integrity, organizations can implement the principle of least privilege and use the BLP model, which allows access based only on the role while issuing credentials to contractors. Moreover, MFA should be compulsory. It will also help maintain the system's availability, and logs should be monitored occasionally to notice any anomalies or discrepancies in the organization. Kerberos can also be implemented, and it is time-based. In terms of risk management, the threat can be mitigated by having some strategies and policies such as regular auditing, real-time log monitoring, incident response plans for 3rd party misuse, Strong Authentication, etc., which will be helpful to prevent any unauthorized access.

G. Malware Risks from Third-Party Software

Another significant threat arising from 3rd party vendors is the introduction of malware via compromised software or tools that 3rd party vendors supply. The tools and applications that these vendors provide are essential for organizations. Threat actors can infect their tools by injecting malicious code into software and applications, posing a huge risk to an organization, as these could lead to zero-day exploits.

A real-life example was the VSA supply chain attack in 2021, where threat actors exploited unknown vulnerabilities (Zero-day vulnerabilities) to inject ransomware into the software. It affected a lot of service providers, and there was a global downtime and disruption in service. (CISA, 2021). These attacks can impact the integrity and availability of the system, leading to data breaches, data loss, and disruption in business continuity. Organizations might also face legal action under the Privacy Act 1988 and the Notifiable Data Breaches (NDB) scheme.

Countermeasures to maintain confidentiality and integrity include a defense-in-depth strategy so that if there are multiple layers of security, it will be hard to bypass, and data should be encrypted when it is in transit and at rest. For availability, organizations should perform audits and log analyses from time to time.

To mitigate risks against threats, vendors should be assessed for security. Applying an access control matrix and applying network segmentation can reduce its impact. By using can tactics, organizations can deal with these types of threats.

H. Loss or Misplacement of Sensitive Client Data

Physical tape backup theft or misplacement poses a serious threat to the data processing department and could have serious ramifications if no countermeasures are implemented. The client's data gets backed up onto tapes and left on open racks in the data processing room. A similar attack happened to Facebook in which a thief stole an unencrypted hard drive filled with 29,000 Facebook employees' information (Lee, 2019). Such an attack would harm the business's reputation, and the affected individuals will be notified as per the NDB scheme. Under the Notifiable Data Breaches (NDB) scheme, any organization or agency that the Privacy Act 1988 covers must notify affected individuals and the OAIC when a data breach is likely to seriously harm an individual whose personal information is involved (OAIC, 2023).

Countermeasures to protect the data using the CIA triad include encrypting all backups to ensure confidentiality. Storing the tapes in a secure and locked location, only available to those who need access, ensures their availability. Maintaining logs on where and what backups are being used ensures the integrity of the files and allows for efficient tracking of the backups in cases where theft occurs.

I. Inadequate Role-Based Access Control (RBAC) Implementation

Improper implementation of Role-Based Access Control (RBAC) exposes Cyber Sentinel Inc. to the risk of privilege misuse, data leakage, and unauthorized system changes. Without clear RBAC enforcement, staff may retain access to systems or data that are unnecessary for their roles. For instance, developers could access live financial systems, or terminated employees may retain dormant credentials with elevated permissions. Misconfigured RBAC systems can lead to insider threats, system compromise, and reputational damage, especially when least privilege is not enforced.

Involving legislation, failure to properly restrict access to personal or sensitive information may violate obligations under the Privacy Act 1988, which mandates that organisations take reasonable steps to protect personal data from unauthorized access or disclosure. Under the Notifiable Data Breaches (NDB) scheme, if a breach is likely to result in serious harm, it must be reported to the affected individuals and the Office of the Australian Information Commissioner (OAIC, 2023). Furthermore, under the Corporations Act 2001, directors and officers could be held accountable for negligence if appropriate risk controls, such as RBAC policies, are not in place or monitored effectively (Australian Government, 2001).

Countermeasures using the C.I.A. triad include restricting access strictly based on job roles and regularly auditing those permissions to ensure confidentiality. Enforcing the principle of least privilege ensures that users have only the access necessary for their roles. For integrity, all access logs should be maintained and reviewed regularly to detect unauthorized changes or anomalies. Regarding availability, critical access roles should include fallback authorizations, but only through secure, documented exception handling procedures. Implementing a centralized Identity and Access Management (IAM) system helps automate RBAC enforcement and improves auditability across the organisation.

4.3.1 Summary of Human-Centric Threat Findings

Cyber Sentinel Inc.'s human-centric threat analysis highlights the significant role that internal users, external personnel, and human behavior play in shaping the organization's security posture. The following conclusions reflect key vulnerabilities identified across departments, alongside their potential impacts and recommended mitigation strategies:

- **Insider threats**, including privilege misuse and intellectual property theft, pose long-term risks due to the trusted access internal staff holds. These threats often go undetected and can lead to serious legal consequences under acts like the Australian Copyright Act and Privacy Act. Addressing them requires layered security controls, insider threat programs, and ongoing staff awareness.

- **Poor cyber hygiene** such as password reuse, unsecured devices, and lack of phishing awareness continues to undermine technical defenses. Tackling this issue demands an organizational culture of shared responsibility, regular education, and enforcement of secure habits.

- **Phishing and social engineering attacks** primarily target internal staff in administrative or privileged roles. These tactics can lead to data breaches, service disruption, or financial loss. Protection efforts must include staff training, technical safeguards like DMARC/SPF/DKIM, and continuous monitoring.

- **Misconfiguration of IT systems** by support staff creates exploitable vulnerabilities across firewalls, user roles, and backup systems. Reducing these risks calls for policy-based automation, regular audits, and secure configuration standards.

- **Delayed security patching** places ongoing projects and critical systems at risk. Manual patching without structured processes increases the likelihood of vulnerabilities being exploited. Recommended actions include automated patching, server backups, patch testing environments, and change control policies.

- **Credential misuse by third-party contractors** introduces risks through over-permissioned access and external attack surfaces. Contractors should be assigned access based strictly on their roles, with controls like MFA, monitoring, and role-based access to ensure protection of sensitive client data and organizational systems.
- **Malware from third-party software** can cause operational disruption, data compromise, and reputational damage. Cyber Sentinel Inc. must adopt a vendor risk management approach, enforce access control, and assess all third-party software before deployment.

- **Inadequate Role-Based Access Control (RBAC)** allows internal or external users to retain access to resources beyond their scope of responsibility, increasing the risk of insider threat, data leakage, and non-compliance. Enforcing strict RBAC policies, conducting privilege audits, and integrating IAM tools will help reduce this risk.

Together, these findings demonstrate the need for a balanced approach that combines technical safeguards with strong human-focused policies, education, and accountability. Cyber Sentinel Inc. must continue to foster a security-aware culture that equips both internal staff and external personnel with the tools, knowledge, and oversight necessary to uphold the confidentiality, integrity, and availability of all information assets.

4.4 Processes and Procedures Threats

A. Lack of Standardized Onboarding and Offboarding Procedures

In the current organization scenario, there is no formal offboarding process to ensure that employee access to digital systems, emails, and physical areas is revoked promptly after termination or resignation. This increases the risk of unauthorized system access by former staff. Additionally, the lack of onboarding procedures regarding NDA imposes a weakness in the company's existing onboarding procedures. Given the sensitivity of ongoing projects in the research and development unit, new staff are required to sign non-disclosure agreements (NDAs), which are legal contracts that prevent them from sharing confidential business information or trade secrets with unauthorized parties (Moghadam & Nejad, 2012).

According to a NASDAQ OMX Corporate Solutions news release (2021), organizations can significantly strengthen their offboarding procedures by enabling IT teams to automate key actions, such as transferring files to a manager when an employee exits. This approach ensures that former users are swiftly removed from all necessary systems and applications, minimizing security gaps and human error that often occur in manual processes.

The legal implications of this threat, such as failure to promptly revoke system access or apply access control during staff transitions, may result in unauthorized access to sensitive data. Under the Australian Privacy Act 1988, organizations must take reasonable steps to protect personal information. If a breach happens and ex-employees still have access, the organization needs to report it under the Notifiable Data Breaches (NDB) scheme. Also, the Corporations Act 2001 states that directors can be held responsible if they fail to manage access properly when the risks are known (Australian Government, n.d.).

A **Mandatory NDA Policy** for all confidential project-related roles:

- Require NDA signing during onboarding.
- HR and legal departments manage NDA signatories for annual review.

Additionally, a **User Access Lifecycle Policy** must be implemented as a countermeasure against the weakness of the offboarding procedure, which includes:

- Formal onboarding and offboarding procedures are integrated with existing HR and IT systems.
- A checklist for immediate access revocation within 24 hours of termination.
- Periodic access audits to ensure only active staff retain access.

Technical enforcement can support this policy through an Identity and Access Management (IAM) system that logs, tracks, and automates account provisioning and deactivation.

B. Lack of Cybersecurity Awareness and Training

According to Sabillon et al. (2019), traditional cybersecurity awareness programs often fail to effectively change employee behavior, leaving human error a significant vulnerability in organizational security. In the current business scenario, there is an apparent lack of formal guidance on what internal staff can or cannot do with company systems, namely using USBs, personal emails, and external apps. In parallel, internal staff use personal laptops, smartphones, or USB devices for work without governance, security checks, or oversight. Considering other implications of the lack of cybersecurity awareness training, primarily from product and sales staff, they may post about projects, clients, or workplace activities without guidance or approval.

An effective cybersecurity awareness program should provide training aligned with the organization's increasing awareness during employees' daily tasks and encourage communication among all parties involved in cybersecurity. Such programs often fail if they do not successfully influence behavior or produce positive

results for the organization. Cybersecurity awareness is a long-term investment essential for building a strong security culture, especially when training is ongoing, and its purpose should extend beyond simply preventing cybersecurity incidents (Sabillon et al., 2019)

The legal implications of failing to implement regular cybersecurity awareness training increase the risk of staff falling for phishing, social engineering, or accidental data breaches. If these incidents involve personal information, they may violate the Australian Privacy Act 1988, which requires organizations to take reasonable steps to protect data. Similar to other identified threats, serious breaches may need to be reported under the Notifiable Data Breaches (NDB) scheme. Public statements without proper oversight can harm the organization's reputation or lead to legal issues. Under the Corporations Act 2001, directors may be held responsible if such actions impact stakeholders or business integrity.

As a countermeasure, the company must implement a **Cybersecurity Awareness and Education Policy** to improve overall security culture and preparedness across all levels, which includes:

- Mandatory cybersecurity training during onboarding and every six (6) months thereafter for all staff.
- Regular simulated phishing campaigns to test and improve employee response, tailored to department-specific context.
- Targeted awareness refreshers for higher-risk roles such as finance, HR, and top executives.

To address the use of company IT systems, a mandatory **Acceptable Use Policy**:

- AUP must be signed during onboarding and reviewed annually.
- All records of violations are logged and reviewed by HR and IT departments.

On the use of personal devices, a **BYOD (Bring Your Own Device) Policy** outlining what personal devices can be used, minimum security standards, and access restrictions:

- Device registration and approval are required before accessing company networks or data.
- Enforcement of security requirements such as encryption, password lock, and updated antivirus software.
- Enable remote wipe capability with the consent of all staff members (in the case of lost or stolen devices).

C. Absence of Formal Change Management Policies

The Office of Technology Services for the Louisiana Division of Administration defines change management policy as a standard that describes the procedures for and specifies the rules and levels of authorizations required to approve different changes. Changes are defined as adding, modifying, or removing a configuration item that could affect IT Services (*Change Management Policy*, 2020). The IT support team can change the server room, network switches, user endpoints, and backup systems without mentioning a documentation process or formal reviews. Without formal reviews or tracking of said changes, errors and threats can occur, such as misconfiguring firewalls, delaying updates, or servers being tampered with.

In addition, the existing business scenario has no formal process exists to test, approve, or document software or system changes in active research and development projects. The research and development staff work on live environments using virtual machines with varied OS setups. Without structured change management, untested code or configurations could be pushed into live and operational environments, resulting in significant business repercussions of system instability, data loss, and potential service-level agreements (SLAs) breaches.

In the ongoing research and development projects, the absence of structured change control increases the risk of system instability and data issues. Mohan et al. (2008) highlight integrating Software Configuration Management (SCM) and traceability to support effective change management. SCM helps control and document changes to software components, while traceability allows teams to track how changes affect different parts of the project. Without these practices, R&D environments may struggle to manage updates properly, leading to fragmented work and unpredictable outcomes.

The legal implications of not enforcing change control and testing in R&D environments include system failures, data loss, and unauthorized exposure of sensitive information. If such failures lead to a data breach, the organization may violate its obligations under the Privacy Act 1988 and be required to report the incident under the Notifiable Data Breaches (NDB) scheme. In addition, under the Corporations Act 2001, directors and officers could be liable for negligence if reasonable project governance and risk management processes were not in place (Australian Government, n.d.).

A **Change Control Policy** must be implemented to reduce the risks caused by unstructured updates in ongoing research and development projects. This includes:

- A formal process for requesting, reviewing, and approving any changes to systems, software, or project components.

- Use clear records to track what changes were made, who approved them, and why the changes were needed.
- Basic change documentation ensures team members see how updates affect other project parts.
- Testing all major changes in a safe environment before they are applied to the live system.

This policy helps maintain project stability and ensures accountability. It must be reviewed regularly and followed by all R&D staff involved in system or software changes of ongoing project developments.

Through the implementation of a change control policy, the organization will be able to stay compliant with the Australian Privacy Act 1988, specifically the Privacy Regulation 2013 act, which requires entities to protect personal data (OAIC, 2023), in this case being personal data relating to companies using the services and software provided.

Additionally, the organization should introduce a **Change Management Procedure** that requires:

- The documentation of proposed changes (Relating to changes to IT Infrastructure)
- A schedule for proposed changes
- Have the proposed changes peer-reviewed and tested in a controlled environment
- A rollback plan in case the changes cause issues
- A post-change review to ensure no complications

To further support the Change Management Policy, the IT support team can use a ticketing tool to keep track of the changes being made, allowing for a traceable method of knowing who requested changes, along with the above-stated documentation.

D. Lack of Routine Privilege Audit and Oversight

Currently, the organization states that from the server rooms to the desktop environments, the IT staff, including IT Support, have easy access throughout the day without mentioning an IT policy that does access reviews, active monitoring, or using the least privilege principle. With the IT Support team having privileges that allow access to all IT infrastructure and services, this can lead to threats such as privilege escalation and creep or allow attackers to gain access to dormant accounts (Provos

et al., 2003). If left unresolved, then issues such as abuse of power from IT support could occur, in which attackers could use the elevated privilege in attacks such as stealing data from the servers, and with the lack of audits, could be ongoing for an indefinite time before the organization is alerted.

If the lack of privilege auditing continues, then it is possible the organization could face legal implications if an attack were to occur through privilege abuse or escalation that resulted in a data breach. The breach of personal information would lead to Notifiable Data Breaches (NDB) forms needing to be sent to the Office of the Australian Information Commissioner (OAIC, 2024).

In order to prevent this, the organization must implement a **Privilege Management Policy** that ensures the following:

- Roles and responsibilities are clearly defined for access levels
- Access reviews are conducted every other month, and privileges must be justified if needed
- Active monitoring in place of those with privileged controls
- Dormant accounts are automatically flagged and disabled
- Privileged accounts must have multi-factor authentication

Furthermore, by implementing the least privilege principle when defining the access levels for the IT support and new accounts, the policy will ensure that accounts will only have access to what they need and nothing more; this can prevent attackers from privilege escalation and in-house attacks from privileged users. Users may be discouraged from committing violations with active monitoring, knowing their requests are being tracked. Tracked actions can be used to analyze user behavior and discover possible or actual violations (Sandhu & Samarati, 1994).

E. Weak After-Hours Access and Visitor Management Process

The existing procedure for approving and documenting after-hours access requests managed by security guard officers at the basement Security Office poses a risk to foolproof security. Vendors and contractors may request after-hours building access, which the Security Office grants without a formal process for verifying the person's identity. The impacts could be the risk of theft of IT hardware or the installation of malicious devices or software/applications that can cause harm to the infrastructure of the organization. Moreover, there are chances of Data exfiltration as well, and most of these can occur during non-operational hours

The legal implications of this threat, including insufficient identity verification or logging of after-hours access, could lead to unauthorized entry into restricted areas such as server rooms or data processing facilities. If personal or client data is accessed or compromised, the organization may breach the Privacy Act 1988, with additional reporting duties under the NDB scheme. Furthermore, the lack of physical access control procedures may be considered a governance failure under the Corporations Act 2001, particularly if senior leadership did not implement appropriate oversight over after-hours operations (Australian Government, n.d.).

A **Physical Access and After-Hours Entry Policy** to address uncontrolled access to secure areas after business hours, which includes:

- Mandatory written approval from department managers for any after-hours building or floor access.
- ID presentation and verification of all visitors and issuance of a temporary visitor/contractor badge are logged at the Security Office.
- Security guards maintain a sign-in and sign-out register.
- CCTV verification if necessary.

Security officers must be trained in the policy, and facilities management should review all records weekly. Emergency override access must be authorized by a senior officer on call. Furthermore, there should be a quarterly compliance audit, and they should follow ISO standards (ISO 27001:2013) for third-party controls (Briasmitatms, n.d.). Also, background checks should be on all contractors and 3rd party vendors. They can also implement time-bound RFID cards to access cards, so they can be allowed access in their area as per their role. They should also be escorted, and logs should be analyzed occasionally.

Another threat can occur due to inadequate monitoring of external visitors while they enter or exit the organization. When visitors, such as clients and auditors, are escorted upon arrival, the lack of enforced entry/exit protocols might lead to unauthorized access to restricted zones such as server rooms. Tailgating could also occur, in which threat actors may enter by following visitors and gain access by acting legitimately. Moreover, the visitors who are connecting their devices to the guest WIFI network may pose a risk of malware infiltration. Another reason could be an inadequate screening of the visitors, in which their identity is not verified correctly, which could lead to their unauthorized access. The impacts could be theft of intellectual property and data breaches.

Regarding the legal implications, it will violate Section 183 of the Corporations Act 2001 for breaching confidentiality (*Federal Register of Legislation*, n.d.) and violate the Privacy Act 1988 if data is compromised (*About PSPF*, n.d.). Moreover, there can

be hefty fines, which can damage the organization's reputation. The countermeasures could be implementing a visitor access and monitoring policy, in which we can implement exit/entry conditions to access biometric access and Real-time RFID cards. Moreover, escorts should be mandatory for all high-risk areas, and alarms should be activated if any unauthorized person accesses them. Also, there should be monitoring via CCTV as well. If these rules are implemented, then this threat can be fixed.

4.4.1 Summary of Processes and Procedures Threats Findings

Cyber Sentinel Inc.'s analysis of policy and procedural threats highlights several structural weaknesses that, if left unaddressed, could result in significant legal, operational, and reputational consequences. Policies serve to establish expectations, while procedures provide step-by-step instructions to ensure consistent and secure staff behavior. The absence or weakness of these controls exposes the organization to unnecessary risks, particularly in the areas of access control, governance, and incident response.

- The **lack of standardized onboarding and offboarding procedures** presents a serious threat to access control, NDA compliance, and data confidentiality. Without a formal process, accounts may remain active after termination, and sensitive information may be accessible beyond employment periods. A User Access Lifecycle Policy and Mandatory NDA Policy are essential to address these gaps and ensure legal compliance under the Privacy Act 1988.

- The **absence of cybersecurity awareness training** contributes to risky user behavior such as falling for phishing attacks, poor device hygiene, and unmanaged communication via social media. The organization must formalize policies on Cybersecurity Awareness, Acceptable Use, Bring Your Own Device (BYOD), and Social Media Use. These policies help reduce human error and ensure long-term legal and security alignment.

- The **lack of structured change control** in research and development projects increases the risk of unstable systems, data loss, and untracked changes, which may lead to legal and contractual breaches. A Change Control Policy must be implemented to enforce pre-approval, traceability, and documented deployment in all ongoing projects.

- The **absence of a broader Change Management Policy** creates vulnerabilities in IT infrastructure by allowing undocumented changes. Policy-backed change documentation, peer reviews, ticketing systems, and backup plans are necessary to establish accountability and protect against configuration errors or unauthorized modifications.

- Without a **Privilege Audit Policy**, excessive or outdated permissions may remain unnoticed, enabling insider abuse or privilege escalation by threat actors. Implementing regular access reviews, privilege monitoring, and automation ensures that privileges are controlled and aligned with the least privilege principle.

- **Weak after-hours access procedures** for contractors and vendors present risks of unauthorized access and unmonitored activities within company premises. Written approvals, strict identity verification, and continuous surveillance through CCTV are necessary controls to prevent potential breaches during low-supervision hours.

- **Improper visitor management practices**, including a lack of logging and verification systems, may result in unauthorized physical access to sensitive areas. Implementing biometric and RFID-based access, alongside CCTV monitoring, can prevent intrusion and reduce liability under the Corporations Act 2001 and the Privacy Act 1988.

In conclusion, the development and enforcement of clear, standardized, and enforceable policies and procedures are critical to strengthening Cyber Sentinel Inc.'s security governance. Formal documentation, coupled with periodic reviews and staff education, ensures that the organization remains compliant, operationally resilient, and prepared to face evolving threats.

5.0 Risk Assessment

5.1 Organizational Information Assets

IT System Component	Risk Management Component	Example Organizational Asset
People	Internal Employee	Employees, System Administrators, Security Team (Physical and InfoSec personnel)
	External Personnel	Contractors and Third-party Vendors
	Trusted Employees	CIO, CSO, R&D Team Members, CEO, Chief Information Technology Officer, Director Sales & Product, Director - Back Office, Legal Officer, Division Head - Research and Development, Division Head - Software Division, Head - Data Processing Division Head - Service and Technical Support, Manager Building and Maintenance, Manager Officer Administration, Manager Finance, Manager Human Resource, Manager Legal Department
	Other Staff Members	Marketing, Sales, Finance Departments, Server Team Network Team Desktop Support Team
	Strangers	Hackers, Phishers, Social Engineers
Procedures	Standard Procedures	User Access Protocols, Strict Password Policies, RBAC, Backup and Recovery Procedures
	Sensitive Procedures	IR plan, DR Plans
	Process Gaps	Lack of Onboarding/ Offboarding Process

Data	Data/Information	Client PII, Financial Records, R&D Prototype Data
	Transmission	Remote Testing of Prototypes, Email Communications
	Processing	Data Analysis for Client Projects
	Storage	Cloud Storage, On-Premises File Servers and Backup Tapes, Client Database (PII and IP Data)
Software	Applications	Email Systems, SIEM tools
	Operating Systems	Windows Server, Linux VM, MacOS
	Security Components	Anti-Virus Software, Firewalls, IDS/IPS
Hardware	Systems & Peripherals	Laptops, Desktops, Servers, USB Devices
	Security Devices	Biometric Scanners, CCTV Cameras
Networking	LAN Components	Routers, Switches, Wireless Access Points
	Intranet Components	Internal Web Portals, File Shares
	Internet/Extranet Components	VPN, Cloud Services, Remote Access Tools
	Cloud-Based Components	Cloud Backup Services, SaaS Platforms

5.2 Asset Classification Scheme

Organizational Asset Classification

IT System Component (Information Asset)	Data Classification	Impact to Profitability
People		
System Administrators / Security Team (Internal Personnel)	**Confidential**	**Critical**
Third-Party Vendors / Contractors (External Personnel)	**Confidential**	**High**
Management, CIO, CSO, R&D Team (Trusted Employees)	**Confidential**	**Critical**
General Employees (Sales, Marketing, HR)	**Private**	**Medium**
Strangers (Cybercriminals / Hackers / Social Engineers)	**Public (Threat Actors)**	**Critical (Risk Impact)**

Procedures		
User Access Management, Password Policies	**Private**	**High**
Incident Response, Disaster Recovery, Patch Management	**Confidential**	**Critical**
Change Control, Onboarding/Offboarding (Process Gaps)	**Confidential**	**Critical**
Data		
Client Data (PII, Financial Records)	**Confidential**	**Critical**
Research & Development Data (IP, Prototypes)	**Confidential**	**Critical**
Internal Business Data (Reports, Logs, Policies)	**Private**	**High**
Backup Data (Onsite / Offsite / Cloud Storage)	**Private**	**High**
Software		
Business Applications	**Confidential**	**High**
Operating Systems (VMs, Authentication Servers)	**Confidential**	**Critical**
Security Tools (Firewalls, IDS/IPS, Antivirus)	**Confidential**	**Critical**
Hardware		
Endpoints (Laptops, Desktops, Mobile Devices)	**Private**	**High**
Servers & Storage Devices	**Confidential**	**Critical**
Security Hardware (CCTV, Access Control Devices)	**Private**	**Medium**
Networking		
LAN Infrastructure (Routers, Switches, Wireless APs)	**Confidential**	**Critical**
VPN & Remote Access Systems	**Confidential**	**Critical**
Internet Connectivity & Cloud Services	**Public / Private**	**Critical**

5.3 Weighted Factor Analysis

Information Asset	Impact on Revenue (40%)	Impact on Profitability (40%)	Impact on Public Image (20%)	Weighted Score (100%)
Client Data (PII, Financial Info)	1.0 × 40 = **40**	1.0 × 40 = **40**	1.0 × 20 = **20**	**100**
R&D Prototype Data (IP)	1.0 × 40 = **40**	1.0 × 40 = **40**	0.8 × 20 = **16**	**96**
Network Infrastructure (LAN, VPN)	0.9 × 40 = **36**	0.9 × 40 = **36**	0.8 × 20 = **16**	**88**
Authentication Servers / OS	1.0 × 40 = **40**	0.9 × 40 = **36**	0.8 × 20 = **16**	**92**
Backup Systems (Recovery)	0.8 × 40 = **32**	0.8 × 40 = **32**	0.7 × 20 = **14**	**78**
Business Applications (CRM/Email)	0.8 × 40 = **32**	0.8 × 40 = **32**	0.6 × 20 = **12**	**76**
Endpoints (Laptops, Desktops)	0.6 × 40 = **24**	0.6 × 40 = **24**	0.5 × 20 = **10**	**58**
Physical Security Systems (CCTV)	0.4 × 40 = **16**	0.4 × 40 = **16**	0.5 × 20 = **10**	**42**

The Weights are as follows:

- Revenue Impact = 40%
- Profitability Impact = 40%
- Public Image Impact = 20%

Scoring Scale is based on the impact

- 1.0 = Critical Impact
- 0.8 - 0.9 = High Impact
- 0.6 - 0.7 = Medium Impact
- 0.4 - 0.5 = Low Impact

5.4 Threat Identification and Overview

Threat Category	Threat	Examples / Description
Data Security Threats	**Data Breach/ Data Theft**	Unauthorized access to PII, IP theft, accidental data compromise
	Data Interception	Eavesdropping during remote prototype testing, unsafe data transmission which can be intercepted using man in the middle attack.
	Loss or Misplacement of Data	Loss of backup tapes, stolen devices containing sensitive data, Data compromised
Insider Threats	**Privileged Misuse**	Insider access abuse, IP theft, misuse of elevated permissions, confused deputy problem, person with low privilege accessed confidential asset
	Negligent Insider Risk	Poor cyber hygiene, weak password usage, data mishandling, careless compromise of data
Social Engineering	**Phishing Attacks**	Fraudulent emails, credential harvesting, link-based malware, fake urls
	Tailgating & Pretexting	Gaining physical access via bypassing physical access (visitor areas, server rooms)
Malware Threats	**Trojan Horse / Malware**	Malicious USBs, files are drive-by downloads, softwares that might act legit but are malicious
	Ransomware	Lock of company's data for an amount
Service Disruption	**Denial-of-Service (DoS/DDoS)**	Flooding services with high traffic to cause downtime until it crashes as in a DDoS attack millions of requests are send via Botnets
	General Service Downtime	Unplanned outages due to lack of redundancy or maintenance. Impacts the operations
System Vulnerabilities	**Unpatched Systems**	Exploiting outdated OS, VMs, or third-party apps, old systems can compromise data
	Misconfiguration of Systems	Incorrect firewall rules, exposed APIs and System with weak security practices

Third-Party Risks	**Supply Chain Compromise**	Vendor software might have backdoors, compromised drivers, contractor credential misuse of access
	Third-Party Malware Risks	Use of compromised external tools 3rd party tool that can be vulnerable and can cause harm to the company
Backup & Recovery Risks	**Backup Failure / Data Loss**	Inability to recover from cyber incidents due to failed backups and lack of IR plan
Physical Security Threats	**Theft of Devices**	Stolen laptops, USB drives, or external storage devices
	Physical Security Breach	Unauthorized entry into server rooms, bypassing CCTV or access controls protocols
	Rogue Access Points	Unauthorized wireless routers creating backdoors into the network and can perform network infiltration
Environmental Threats	**Power Outages**	Disruption of services due to loss of power
	Thermal Overheating Risks	Server room overheating, HVAC failure
	Natural Disasters	Floods, fires, or other disasters impacting the IT infrastructure
Process & Governance Gaps	**Weak Onboarding/Off boarding**	No structured process for account lifecycle management
	Lack of Change Control	Lack of beta testing or rollback plans for system changes
	Lack of Privilege Audits	Excessive or stale privilege assignments that are not reviewed properly
	Weak Visitor Management	Poor physical control over after-hours access and visitor tracking
	Lack of Cybersecurity Training	Untrained staff vulnerable to social engineering and phishing

5.5 Threat Assessment Criteria

Rank	Asset and Component	Data Classifi-cation / Criticality	Business Impact	Threat Exposure	Risk Justification
1	**Client Data (PII, Financial Info)** – *Data*	Confidential / Critical	Legal and reputational actions can be taken	High	Client data is prone to phishing, social engineering, and data compromise. As per ISO/IEC 27005 standard it emphasizes criticality of protecting sensitive data assets.
2	**Authentica-tion Servers & OS** – *Software/ Systems*	Confidential / Critical	Total system compromises due to credential theft	High	IAM systems are important assets due to its important significance in overall system protection of the organization
3	**R&D Prototype Data (IP)** – *Data/ Software*	Confidential / Critical	Costly IP theft and hard to recover after attack	High	Intellectual property is a high-value target which can cause several impacts to the company in many aspects
4	**Network Infrastru-cture (Routers, VPN, Firewall)** – *Networking*	Confidential & Availability / Critical	Service outages and productivity losses can disrupt operations	Medium	Network infrastructure is essential for availability, with DDoS incidents increasing day by day globally. It is a best practice for patching the system from time to time
5	**Backup Systems (Cloud+ Local)** – *Hardware/ Software*	Private / High	Loss of recoverability; extended downtime, financial loss from ransomware	Medium	Backups are a ransomware target to gain capital from the company. NIST and ISO 27005 recommend immutable, tested backups for the data protection of the company

6	**Business Applica-tions (CRM, Email)** – *Software*	Confidential / High	Core to business operations; compromise of this application will cause major disruption and data exposure	Medium-High	Business applications are common entry points for malware and phishing and can infect the security infrastructure of the company
7	**End-User Devices (Laptops, Desktops, Mobile)** – *Hardware*	Private / Medium	potential data leakage	High	Endpoints are a common target for bad actors as they can insert malware and perform social engineering
8	**Physical Security Systems (CCTV, Access control)** – *Hardware/ Physical*	Private / Medium	Physical access allows theft and tampering, also increases attack surfaces	Low-Medium	Physical security is essential for defense-in-depth strategies are needed to improve the security layers in an organization.
9	**Visitor Manage-ment Process** – *Procedures/ Physical*	Private / Medium	Unauthorized facility access risk, especially after-hours	Medium	As per SANS institute Visitor management is required for compliance and physical security
10	**Server Room Equipment and Environmen tal Controls** – *Hardware/ Physical*	Confidential / High	Direct threats to availability, hardware damage due to heat/power	Medium –	Environmental threats such as power outages are part of ISO 27005 risk management and NIST 800-30 guidance

5.6 Asset Prioritization and Ranking

Category	Threat Type	Priority Rating (1–5)	Reason/ Justification
People	Insider Threat (IP Theft, Privilege Misuse)	**5**	High cost of monitoring, DLP, insider threat detection, audits
	Social Engineering / Phishing	**4**	Requires ongoing employee training, phishing simulations, email filters
	Poor Cyber Hygiene (Weak Passwords, Reuse)	**4**	Requires constant education, enforcement of MFA and password policies
	Misconfiguration of Critical IT Systems	**4**	Internal misconfiguration of firewalls, or backups can lead to critical vulnerabilities
	Delayed/Inconsistent Security Patch Management	**4**	Leads to an increased risk of exploitation, can lead to IT time and cost burden
Procedures	Lack of Change Control / Process Gaps	**4**	Implementation of formal procedures and CCB consumes time & money
	Inadequate Onboarding / Offboarding	**3**	Involves HR-IT collaboration but lower priority compared to cyber threats
	Lack of Routine Privilege Audit and Oversight	**4**	Inactive accounts or excessive privileges introduce insider and escalation threats
	Inadequate Role-Based Access Control (RBAC) Implementation	**4**	Lack of RBAC leads to privilege creep and data exposure risks
	Weak After-Hours Access and Visitor Management Process	**3**	Procedural gaps lead to physical access risks, which can lead to insider threats, high expense
Data	Client Data Breach / IP Theft	**5**	Most critical—high legal, financial, reputational risks
	Backup Failure / Data Loss	**3**	Investment in cloud backups, but not the top everyday expense

Software	Malware / Trojan Infiltration	**5**	High spends on EDR, antivirus, patching systems
	Unpatched Systems / Vulnerabilities	**4**	Ongoing cost for patch management, vulnerability scanning
	Denial-of-Service (DoS) attacks	**4**	Distributed or General DoS attacks require anti-DDoS protection, which is costly, if not acquired, then possible business disruption
	Remote Prototype Testing Data Interception	**4**	Prototype data could be stolen, requires VPNs and secure tunnels
Hardware	Physical Theft / Loss of Devices	**3**	Investment in asset tracking and encryption, but less than cyber controls
	Overheating / Power Failure	**2**	Basic UPS & cooling system investment, but less focus overall
	Unmonitored Access to Critical IT Area	**4**	Tailgating, lack of policy regarding server room and unmonitored APs elevate threats, requires training, policies, possible CCTV
	Power Outages in Critical IT Infrastructure	**2**	Investing in UPS and redundancy will reduce the risk greatly
Networking	DDoS & Network Attacks	**4**	Costly firewalls, anti-DDoS services, network monitoring
	Rogue Access Points / Unauthorized Network Devices	**3**	Requires network audits and rogue AP detection tools
Third-Party / Supply Chain	Vendor Software Risk / Contractor Credentials	**3**	Vendor assessments & third-party risk management are moderate priorities

5.7 Vulnerability Assessment

Threat	Possible Vulnerabilities
Data Breach	Bad data encryption, Very Weak access controls and excessive data permissions to all employees
Insider Threat	Lack of log monitoring and privilege management, no behavioural anomaly detection for the employees
Phishing/ Social Engineering	Lack of training and awareness and failure to verify identities for sensitive requests as its manipulation tactics play with human brain
Malware/Trojan Horse	Bad endpoint security, lack of USB device control
Denial of Service (DoS/DDoS)	Lack of network segmentation, insufficient firewall rules, lack of WAF (Web Application Firewall) , Lack of backup server
Unpatched Systems	No automated patching system, delayed OS and application updates, unsupported old and outdated systems
Misconfiguration of Systems	Open ports, weak Intrusion rules, weak passwords
Third-Party/ Supply Chain Risk	No vendor software security assessment, lack of third-party risk contracts (SLA)
Backup Failure/ Data Loss	Lack of backup testing, no data integrity inspection
Physical Security Breach	Unsafe server rooms, lack of CCTV monitoring, weak visitor tracking
Environmental Threats	No power backup (UPS), poor HVAC maintenance
Privilege Escalation	Lack of RBAC, DAC enforcement, overprivileged user accounts so anyone can play with data
Weak Onboarding/Offboarding	Failure to disable old employee accounts so they can still access company data and poses serious concerns
Change Management Failures	No structured change control process, inadequate testing before deployment, lack of rollback plans
Third-Party Credential Misuse	Shared vendor accounts, no MFA on vendor accounts, inadequate logging of third-party activity
Technological Obsolescence	Use of outdated hardware/software without security updates, unsupported OS
Rogue Access Points	Lack of wireless monitoring, no MAC address filtering, no rogue AP detection tools
Software Vulnerabilities	Use of unverified open-source components, no secure code review, lack of vulnerability scanning
Lack of Cybersecurity Training	Employees unaware of phishing and malware tactics, absence of refresher courses

5.8 Threat-Vulnerability Assessment (TVA) Worksheet

Threat	Category	People	Procedures	Data	Software	Hardware	Networking	Third-Party/ Supply Chain
Unpatched Virtual Machines and Operating Systems	Technical Threats	3		4	5		4	
Data Interception During Remote Prototype Testing	Technical Threats			5	4		4	
Distributed Denial-of-Service (DDoS) Attacks	Technical Threats		3		4		5	
Malware Infiltration via External Devices and Trojan Horse Programs	Technical Threats	3		4	5	4		4
General Denial-of-Service (DoS) Attacks Targeting Availability	Technical Threats			3	3		4	
Unmonitored Access to Critical IT Areas	Physical Infrastructure Threats		4			5	4	
Power Outages in Critical IT Infrastructure	Physical Infrastructure Threats			4	3	4		
Thermal Risks and Overheating in Equipment Rooms	Physical Infrastructure Threats					4	3	
Theft or Loss of Physical IT Equipment	Physical Infrastructure Threats	3		4		5		
Rogue Access Points and Unauthorized Network Devices	Physical Infrastructure Threats					4	5	4
Insider Threats and Privileged Misuse by Employees	Human-Centric Threats	5	4	5				
Poor Cyber Hygiene Practices Across Departments	Human-Centric Threats	4	3		4			

Social Engineering and Phishing Exploits	Human-Centric Threats	4	3	3				
System Misconfigurations by Internal Users	Human-Centric Threats	4	4		5			
Delayed or Inconsistent Security Patch Management	Human-Centric Threats	4	3		5			
Credential Misuse by Third-Party Contractors	Human-Centric Threats	4						5
Malware Risks from Third-Party Software	Human-Centric Threats				4			5
Loss or Misplacement of Sensitive Client Data	Human-Centric Threats	3	3	5				
Inadequate Role-Based Access Control (RBAC) Implementation	Human-Centric Threats	5	4					
Lack of Standardized Onboarding and Offboarding Procedures	Processes and Procedures Threats	4	5					
Lack of Cybersecurity Awareness and Training	Processes and Procedures Threats	4	4					
Absence of Formal Change Control in R&D Projects	Processes and Procedures Threats		5		4			
Lack of Routine Privilege Audit and Oversight	Processes and Procedures Threats	4	5					
Weak After-Hours Access and Visitor Management Process	Processes and Procedures Threats	3	4					

5.9 Risk Control Overview

Resource Item	Control Best Practices	Due Diligence	Considerations	Metrics and Measurements	Measurement In Use
Software	The *Essential Eight* framework by the ACSC (2023) outlines best practices such as patch management, multi-factor authentication (MFA), and malware protection as significant to uphold software security. Additionally, these align with the **NIST Cybersecurity Framework**, which emphasizes secure development and insider threat mitigation (ISO/IEC, 2023). The general best practices for software threat control include: ⇒ Applying a multi-layered protection that includes patch management, endpoint protection, firewall, and data backups. ⇒ Train staff against malware and phishing threats. ⇒ Use secure software development practices and version control in R&D.	Due diligence concerning software-related assets must be upheld by applying critical patches within 48 hours, restricting admin access, and monitoring antivirus updates, which are part of expected due diligence. These practices are recommended by both the ACSC (2023) and the **OAIC** in their guidance for securing personal information (OAIC, 2023). The general due diligence for software threat control include: ⇒ Keeping operating systems and virtual machines updated. ⇒ Deploying antivirus and malware protection regularly. ⇒ Limiting software installation privileges among personnel and staff.	When we consider the controls for threats related to software threats, it is essential to make sure that all the OS and VMs are updated with the latest software and patched from time to time to eliminate vulnerabilities. Moreover, strict access controls such as RBAC, which is based on role, should be implemented to prevent any unauthorized access by threat actors. The legal implications could be the Australian Privacy Act 1988 and Notifiable Data Breaches (NDB) scheme, which suggests that the PII of individuals should be protected from threat actors. Furthermore, the security policies should match the SDLC life cycle and follow the best practices, which will reduce risk and ensure code quality.	The general metrics for software threat control include: ⇒ Patch deployment time. ⇒ The percentage of systems with the latest security patches. ⇒ The number of malware quarantines. ⇒ The number of inventory audits conducted. ⇒ The system uptime. ⇒ In cases of attacks, the attack time.	The measures in use for software threat control include: ⇒ The patch deployment time can be used to create a Patch Compliance Score ⇒ Percentage of devices that have been patched within a period, to measure the efficiency of the patch application process. ⇒ The percentage of systems with the latest patches can be used to measure overall patch compliance. ⇒ The number of malware quarantines is used to measure the number of malwares introduced to the system.

Physical Infrastr-ucture	The **Australian Cyber Security Centre (ACSC)** recommends implementing layered physical security for data centres and server rooms, which includes access control, surveillance, and physical barriers, as part of the *Essential Eight Maturity Model* (ACSC, 2023). In addition, ISO/IEC 27002:2023 presents specific best practices for securing physical infrastructure concerning equipment, rooms, and entry points in an organization's physical environments (ISO/IEC, 2023). ⇒ Applying a layered security on physical barriers (locks, doors), surveillance (CCTV), and Monitoring (access logs). ⇒ Ensuring controlled access to critical server rooms with the use of smart badges or personnel biometrics ⇒ Regularly testing environmental controls (e.g., power, cooling, fire suppression).	Physical access to critical infrastructure must be logged, reviewed, and restricted to authorised individuals. The ACSC (2023) defines due diligence in this context as maintaining locked server rooms, verifying visitor credentials, and implementing environmental Monitoring. These steps also align with recommen-dations in the ISO/IEC 27002:2023 standard. The general due diligence for physical infrastructure threat control includes: ⇒ Maintaining secure access procedures among personnel (sign-in logs, elevating existing escort policies). ⇒ Ensuring fire and environmental safety checks are documented and updated regularly. ⇒ Locking and monitoring all critical IT server rooms and wire racks.	Risk control decisions must be considered when assessing the physical access to the organization's building. This covers after-hours access, facility layout, emergency power, and the organisation's ***duty of care*** under the **Work Health and Safety Act** (Safe Work Australia, 2022). The general considerations for physical infrastructure threat control include: ⇒ After-hours access, maintenance crew controls, emergency protocols, and business continuity in disasters. ⇒ Staff compliance with entry and exit logging.	ISO/IEC 27004:2016 recommends tracking the "*percentage of secure areas with enforced access control*" and the number of "*environ-mental risk alerts*" per period as core physical security KPIs (ISO/IEC, 2016). The general metrics for physical infrastructure threat control include: ⇒ Number of unauthorise d access attempts (personnel badge). ⇒ Frequency of environment al alerts (overheating, power outages). ⇒ Incident response time (historical data).	The measures in use for physical infrastructure threat control include: ⇒ The TVA will be used to map each physical threat to a specific vulnerable asset (e.g., wiring closet) and assess: Risk = (Likelihood × Asset Value) – Existing Controls + Uncertainty Adjustment

People	The general best practices for people-based threat control include: ⇒ Implementing role-based access control (RBAC) and least privilege principles. ⇒ Conducting regular security awareness training ⇒ Requiring multi-factor authentication (MFA) for privileged users ⇒ Monitoring user activity through SIEM tools and maintaining audit trails ⇒ Using exit protocols for employees leaving the organisation ⇒ Fostering a stronger cybersecurity culture	The general due diligence for people-based threat control includes: ⇒ Ensuring all staff receive proper induction training on cybersecurity ⇒ Document and enforce acceptable use policies ⇒ Run quarterly audits of access levels and insider risk assessments ⇒ Conduct background checks on contractors and full-time staff ⇒ Comply with legal obligations under the Australian Privacy Act 1988 and the NDB Scheme in case of any breaches	The general considerations for people-based threat control include: ⇒ Access levels should vary across different roles (e.g., Developer vs. Contractor vs. CSO) ⇒ Insider threats can be both intentional and accidental ⇒ Cultural and language barriers can affect training effectivity	The general metrics for people-based threat control include: ⇒ The percentage of staff completing the security training ⇒ Number of unauthorised access attempts ⇒ Average time to revoke access after staff leave the organisation ⇒ The percentage of accounts with MFA enabled ⇒ How often do user access reviews occur ⇒ Number of unused privileged accounts	The measures in use for people-based threat control include: ⇒ Training Completion Dashboards from the LMS used with the security training ⇒ SIEM logs show the account activity and access anomalies ⇒ Access review reports ⇒ MFA coverage reports measure how many users have it

Processes and Proced-ures	The best practices include: ⇒ The implementation of transparent policies and policies that are based on the roles of the employees, such as Non-Disclosure Agreements (NDAs), Bring Your Device (BYOD) Policy, Change Management Policy, and Acceptable Use Policy (AUP). ⇒ Moreover, standard industry policies such as ISO/IEC 27001:2013 should be implemented. ⇒ Furthermore, the policies shall be checked, updated, and approved from time to time for 6 months to maintain business continuity and compliance with the policies.	To maintain diligence, it's necessary to: ⇒ Ensure that all employees, contractors, and vendors are familiar with company policies, such as NDA and AUP, when they join the company and know the consequences for non-compliance. ⇒ Moreover, organizing Cybersecurity Awareness Training for all the staff members helps maintain cyber hygiene, and maintaining the logs of violations of policies and reviewing them from time to time will help to maintain the proper implementatio n of the policies. ⇒ Records of these should be maintained for auditing.	Considerations are some legal obligations such as the Australian Privacy Act 1988 and the Notifiable Data Breaches (NDB) scheme, which requires organizations to follow the best practices and implement polices to protect the PII of the individuals. Also, the policies should be written in simple language so that all departments of the organization can understand and follow the same, and policies should be created based on the level of access and the risk for each role.	The general metrics for policies and procedures threat control include: ⇒ Tracking the number of signed policies acknowledg-ment forms, frequency of violations, the type of violations of policies, and the action taken. ⇒ Moreover, metrics can be collected by tracking the completion rate of Cybersecurit y Training Programs. ⇒ Monitoring this data occasionally and reporting any discrep-ancies to senior manage-ment is good practice.	The measures that can be used: ⇒ Compliance dashboard that will track the acknowledg ement of the staff, their completion of training, and logging the violations by employees. ⇒ Audits should be performed every 4 months by the compliance team to verify whether policies are followed and what can be improved. ⇒ Results found after analysis can be used to update the policy framework.

5.9.1 Software-Based Threat Controls

Resource Item	Control Best Practices	Due Diligence	Considerations	Metrics and Measurements	Measurement In Use
Unpatched Virtual Machines and Operating Systems	⇒ Patch OS/VMs within 48 hrs ⇒ Version control ⇒ Endpoint protection	⇒ Regular patch testing ⇒ Maintain update logs	⇒ Legacy systems may not support updates ⇒ Non-compliance risk under ASD Essential Eight	⇒ Percent (%) systems patched on time ⇒ Number of unpatched systems	⇒ SIEM admin logs ⇒ Patch status reports
Data Inter-ception During Remote Prototype Testing	⇒ Enforce end-to-end encryption ⇒ Mutual authentication ⇒ VPN or secure tunneling	⇒ Encrypt all test transmissions ⇒ Monitor data transmission routes	⇒ Exposure of client-linked data resulting to legal risk under Privacy Act ⇒ Use of third-party lines (e.g., satellite)	⇒ Number of of interception alerts ⇒ Percent (%) of encrypted traffic	⇒ Encryption enforced end-to-end ⇒ SIEM logs remote traffic anomalies
General Denial-of-Service (DoS) Attacks Targeting Availability	⇒ Use failover systems ⇒ Alert on network spikes ⇒ Maintain updated firewall rules	⇒ Identify normal traffic baselines ⇒ Block known malicious IPs	⇒ Internal tools (e.g., Shake & Quake) risk downtime ⇒ May be mistaken for DDoS	⇒ DoS event frequency ⇒ Average recovery time	⇒ Network logs reviewed ⇒ Alert thresholds calibrated
Distributed Denial-of-Service (DDoS) Attacks	⇒ Use DDoS mitigation services ⇒ Network segmentation ⇒ Load balancing	⇒ Monitor traffic patterns ⇒ Maintain ISP contact protocols	⇒ Impacts Shake & Quake uptime ⇒ Reputatio damage & SLA breach risk ⇒ May mask other attacks	⇒ DDoS attempts per month ⇒ Downtime due to DDoS	⇒ Firewall/WAF logs ⇒ SIEM DDoS analytics ⇒ Monitoring tools auto-alert

Malware Infiltration via External Devices and Trojan Horse Programs	⇒ Auto-scan removable devices ⇒ Use application control ⇒ Endpoint AV protection	⇒ Disable auto-run ⇒ Restrict USB access ⇒ Train users on malware signs	⇒ BYOD policies needed ⇒ Malware can persist post-removal	⇒ Removable media usage ⇒ Number of malware detections	⇒ Antivirus logs reviewed weekly ⇒ USB control enforcement logs

5.9.2 Physical Infrastructure Threat Controls

Resource Item	Control Best Practices	Due Diligence	Considerations	Metrics and Measurements	Measurement In Use
Unmonitored Access to Critical IT Areas	⇒ Implement role-based physical access controls ⇒ Enforce strict visitor escort policies	⇒ Verify access logs weekly ⇒ Audit badge assignment quarterly	⇒ Initial installation costs ⇒ Staff resistance to new authentication	⇒ Percentage of unauthorized access attempts	⇒ Weekly review of badge access logs ⇒ Review of alerts triggered
Power Outages in Critical IT Infrastructure	⇒ Intstall uninterruptible power supplies (UPS) ⇒ Test backup power generators quarterly	⇒ Test UPS systems monthly ⇒ Schedule generator tests ⇒ Document test outcomes	⇒ UPS batteries require periodic replacement ⇒ Generators may require local compliance	⇒ Percentage of UPS system uptime during outages ⇒ Percentage of successful generator tests	⇒ UPS testing results logged and reviewed ⇒ Generator performance audits
Thermal Risks and Overheating in Equipment Rooms	⇒ Deploy wireless thermal sensor networks ⇒ Apply aisle containement strategies	⇒ Daily monitoring of thermal dashboards ⇒ Airflow inspects conducted quarterly	⇒ Wirrless connectivity reliability ⇒ Server room layout adjustments	⇒ Number of temperature threshold breaches ⇒ Thermal sensor logs ⇒ Airflow inspection reports	⇒ Thermal alerts tracked ⇒ Airflow audits reviewed quarterly

Theft or Loss of Physical IT Equipment	⇒ Encrypt all portable devices ⇒ Use cable locks and secure storage	⇒ Encryption compliance audits ⇒ Checks of physical locks	⇒ Encryption impacts device perform-ance ⇒ Cable locks insufficient protection	⇒ Percentage of portable devices encrypted	⇒ Encryption compliance reports ⇒ Cable lock compliance reports
Rogue Access Points and Unautho-rized Network Devices	⇒ Deploy Wireless Intrusion Prevention Systems (WIPS) ⇒ Enforce Zero Trust Architecture ⇒ Regular device audits	⇒ Weekly rogue AP scans ⇒ Audits of connected devices accesses	⇒ WIPS false positives ⇒ Latency from Zero Trust imple-mentation	⇒ Number of rogue APs detected/blocked ⇒ Percentage of unauthor-ized devices removed	⇒ WIPS detection logs review ⇒ Device audit reports results

5.9.3 People-Based Threat Controls

Resource Item	Control Best Practices	Due Diligence	Considerations	Metrics and Measurements	Measurement In Use
Insider Threats and Privileged Misuse by Employees	⇒ Role-based access control (RBAC) ⇒ MFA for privileged users ⇒ Monitor privileged activity via SIEM	⇒ Conduct regular audits ⇒ Revoke access upon employee exit ⇒ Least privilege access	⇒ Can be intentional or accidental ⇒ Legal risks under NDB	⇒ Number of privilege misuse alerts ⇒ Time to revoke access	⇒ Audit logs reviewed quarterly ⇒ SIEM detects and alerts anomalies
Poor Cyber Hygiene Practices Across Departments	⇒ Enforce security awareness programs ⇒ Set clear acceptable use policy (AUP)	⇒ Track training participation ⇒ Enforce BYOD and clean desk policy	⇒ Departmenta l gaps in compliance ⇒ Influenced by culture and role	⇒ Training completion rates ⇒ Policy violations per dept.	⇒ LMS dashboard monitors training ⇒ Reports reviewed monthly

Social Engineering and Phishing Exploits	⇒ Phishing simulations ⇒ Security awareness workshops ⇒ Email filtering	⇒ Encourage reporting of suspicious emails ⇒ Update staff directory policies	⇒ Human error is the weakest link ⇒ Tailored attacks likely	⇒ Phish test success rates ⇒ Response time to reports	⇒ Simulations conducted quarterly ⇒ Reports reviewed by CSO
System Miscon-figurations by Internal Users	⇒ Regular firewall and configur-ation audit ⇒ Policy based automation tools	⇒ Configuration reviews ⇒ Monthly verification of automation compliance	⇒ Staff pushback from audits ⇒ Automation setup costs	⇒ Percentage reduction in configur-ation errors	⇒ Monthly configur-ation audit reports reviewed ⇒ Automation success rates reviewed
Delayed or Inconsistent Security Patch Manage-ment	⇒ Enforce routine patch schedules ⇒ Sandbox patch testing	⇒ Patch testing logs reviewed prior to deployment ⇒ Compliance reports	⇒ Testing delays postponing critical patches ⇒ Compatibilit y issues with legacy systems	⇒ Percentage of systems patched in SLA timeline	⇒ Patch testing reports ⇒ Weekly patch success tracking ⇒ Monthly SLA compliance reports
Credential Misuse by Third-Party Contra-ctors	⇒ Strict RBAC ⇒ Enforced MFA ⇒ Contractor activities monitored	⇒ Quarterly RBAC audits ⇒ MFA compliance checks ⇒ Real-time contractor sessions monitored	⇒ Contractor onboarding sessions ⇒ Clear offboarding processes required	⇒ Percentage of contractor account with MFA ⇒ Percentage of deact-ivated contractor accounts on time	⇒ RBAC and MFA compliance reports ⇒ Contractor access logs ⇒ Monthly review of contractor activity
Malware Risks from Third-Party Software	⇒ Deploying EDR Software audits, use the software that is needed in the organization	⇒ Validating the supplier of the software and the contract with the company, also to review the software inventory from time to time	⇒ Supply chain could be compromise d, and it is posing a risk for 3rd party zero day	⇒ Percentage of approval of third-party software.	⇒ Review of software every 4 months and Logs should be analyzed as well from time to time.

Loss or Misplace-ment of Sensitive Client Data	⇒ Enforce Data Encryption in AES 256 ⇒ Implement DLP ⇒ Keep data updated in cloud	⇒ Review DLP Policies time to time ⇒ Client Data Monitoring from time to time	⇒ It can damage the reputation of the company and should follow GDPR best practices	⇒ Percentage of DLP incidents	⇒ Monthly review of DLP and IR
Inadequate Role-Based Access Control (RBAC) Implemen-tation	⇒ Enforcing RBAC policy Using automated tools for access based on the job	⇒ Regular access audits time to time ⇒ Verifying the privilege of every employee	⇒ Risk of privilege escalation and Disruption to operation could occur	⇒ Percentage of RBAC defaulters	⇒ Automated RBAC reports monthly to analyze any intrusion. ⇒ Checking the logs every month.

5.9.4 Process-Based Threat Controls

Resource Item	Control Best Practices	Due Diligence	Considerations	Metrics and Measurements	Measurement In Use
Lack of Stand-ardized On-boarding and Off-boarding Procedures	⇒ Follow the best industry standards and protocols for onboarding. Automating the User Account lifecycle management	⇒ Conducting Regular reviews of the Process	⇒ Risk of Unauthorize d access	⇒ To deactivate account once an employee leaf	⇒ Monthly review of deactivation logs
Lack of Cyber-security Awareness and Training	⇒ Compulsory training for all the employees, also to organize phishing simulations time to time	⇒ Tracking of the training and updating training modules based on the emerging trends	⇒ It can be hard to participate remotely, and some staff might not have any technical knowledge	⇒ Tracking of Completion Rate of the training	⇒ Monthly reports of performance analyzed by higher authority

Absence of Formal Change Control in R&D Projects	⇒ Implement change management policy	⇒ Maintaining a log for changes	⇒ There can be risk of any unauthorized changes	⇒ Percentage of unapproved and approved changes	⇒ Monthly meeting for change controls
Lack of Routine Privilege Audit and Oversight	⇒ Fortnightly audits of privilege access and implement the principle of least privilege	⇒ Updating and maintaining the privileges from time to time	⇒ Insider threat risk that could lead to zero day	⇒ Percentage of employees that have acess and its violators	⇒ Log review from time to time ⇒ SOC will also detect any issue
Weak After-Hours Access and Visitor Manage-ment Process	⇒ Implement strict security after hours, Using electronic visitor System	⇒ Permission needed to access the after hours	⇒ Increased physical security so only people with authority can enter	⇒ Visitors who are going after hours should enter their name and id	⇒ Logs are reviewed weekly by the physical security team

6.0 Risk Management

The following risk treatment strategies and their corresponding definitions are directly adapted from Whitman and Mattord's Management of Information Security (2018). These terms are used throughout the Risk Assessment and Control sections for Cyber Sentinel Inc. to ensure consistency and alignment with established infosec management practices.

Acceptance	*Understanding the consequences of choosing to leave an information asset's vulnerability facing the current level of risk, but only after a formal evaluation and intentional acknowledgment of this decision.*
Avoidance	*Applying controls and safeguards that eliminate or reduce the remaining uncontrolled risk. This approach is sometimes referred to as the defense strategy*
Mitigation	*Reducing the impact to information assets should an attacker successfully exploit a vulnerability.*
Transference	*Shifting risks to other areas or to outside entities.*

6.1 Treatment Options and Justification

Technical Threats (Software and Systems)		
Threat Item	**Best Approach**	**Alternative Approach**
Unpatched Virtual Machines and Operating Systems	**Mitigation** The best practice would be risk mitigation, which includes the implementation of routine patch management, conducting audits to keep the system up to date, and hardening the virtual environments by isolating the critical systems, controlling access based on roles, and scanning the VM images to check for any discrepancies.	**Avoidance** Moreover, an alternative approach can avoid risk, but it is less practical as replacing all the systems is a good idea to make them secure. Still, it will cost the organization a lot and cause downtime, so risk mitigation is the best practice for now. Also, enabling policy-based updates can fix this issue.
Data Interception During Remote Prototype Testing	**Mitigation** The best way to manage this risk is through mitigation. While remote prototype testing is essential and cannot be avoided, the risk of data interception can be significantly reduced with affordable solutions. These include using end-to-end encryption such as SSL or VPNs, requiring strong	**Transference** Another option the organization can explore for this risk is transference. This involves outsourcing secure prototype testing to a trusted third-party provider or using cloud platforms offering built-in data transfer encryption. Doing such practice shifts most security

	authentication for remote access, and logging all sessions to monitor data transfers. This method allows important R&D work to continue while protecting sensitive information and client data. According to the Threat–Vulnerability–Asset (TVA) model, the asset is valuable, and the threat is real, but the vulnerability can be lowered with practical controls. In a setting with limited resources, mitigation is realistic and valuable, allowing the organization to continue vital work while minimizing risks.	responsibility to the service provider, often with added protection through service-level agreements. Although this approach increases dependence on external vendors, it can be a practical alternative if in-house mitigation becomes too demanding on resources.
General Denial-of-Service (DoS) Attacks Targeting Availability and Distributed Denial-of-Service (DDoS) Attacks	**Transference** Transference is the most suitable approach for managing this risk. Defending against DDoS attacks typically requires costly infrastructure and 24/7 monitoring, which may be beyond the capabilities of a smaller organization. The business can access advanced security features such as traffic filtering, threat detection, and scalable defense systems by outsourcing protection to specialized providers like Cloudflare, AWS Shield, or the organization's current ISP. This strategy shifts much of the risk and responsibility to a third party with the necessary expertise and infrastructure. It helps maintain service availability while preserving internal resources for essential functions.	**Mitigation** An alternative strategy the organization can adopt is mitigation by applying internal security measures. These may include setting rate limits on incoming web traffic, using firewall rules to block suspicious IP addresses, and adjusting server timeout settings. Although these steps may not fully protect against large-scale DDoS attacks, they can help lessen the impact of more minor incidents and provide a basic defense layer in situations where external protection services are not accessible or feasible.
Malware Infiltration via External Devices and Trojan Horse Programs	**Mitigation** The recommended strategy for managing the risk of Trojan Horse Malware is mitigation. This includes deploying antivirus software, implementing email filtering, and providing cybersecurity training to raise staff awareness. Restricting software installation through least privilege access and enforcing a Bring Your Own Device (BYOD) policy further reduce exposure. These controls strike a balance between cost and protection. Given the widespread nature of malware, transferring or accepting the risk is not realistic investing in preventive measures is the most effective approach.	**Avoidance** Alternatively, the other option would be to avoid the risk of Trojan horse malware. To do so, the organization would need to enforce a BYOD policy, as stated above, to prevent staff from compromising the system through a device lacking security measures. Avoid using third-party software, which would be very disruptive to the system. Furthermore, to avoid the risk entirely, the organization would have to stop using the internet, which is unrealistic. For these reasons, while avoiding is the alternative option to mitigating, it is still far worse than investing the money in mitigating the risk.

Physical Infrastructure Threats		
Threat Item	**Best Approach**	**Alternative Approach**
Unmonitored Access to Critical IT Areas	**Mitigation** The best way to address the risk of unmonitored physical access to critical IT infrastructure is through mitigation. These areas, including server rooms and wiring racks, often house vital equipment and must remain protected from unauthorized individuals. This can be done with affordable physical security measures such as smart access systems (keycards or biometrics), locked doors, visitor sign-in procedures, and regular reviews of access logs. These steps promote accountability and limit access without significant costs. Clear access policies and employee training also help prevent internal mistakes that could expose the physical infrastructure.	**Transference** If implementing mitigation controls internally is not feasible due to staffing or equipment limitations, the organization can choose transference by outsourcing physical security to a third-party provider. External security teams or building management can handle access control, enforce policies, and maintain visitor logs. This shifts responsibility to specialists and can offer stronger oversight when defined in a service-level agreement. While this option is practical, it requires careful contract management and is often better suited to larger or higher-risk environments.
Power Outages in Critical IT Infrastructure	**Mitigation** Mitigation is the most practical way to manage power disruptions in server rooms and data infrastructure. Although outages are unpredictable, their impact can be reduced with uninterruptible power supplies (UPS), surge protectors, and basic backup systems. These tools provide short-term power continuity and allow time for safe system shutdowns to prevent data loss. Regular maintenance and testing of electrical systems also help lower the risk. Since these solutions are affordable and scalable, they are well-suited for organizations with limited resources.	**Transference** If maintaining even basic backup systems is financially demanding, the organization could transfer the risk by moving critical services to a third-party cloud provider or data center. These providers usually offer built-in power redundancy and high availability as part of their infrastructure. This shift places the responsibility for power reliability on the vendor. However, this approach also means relying on the provider's infrastructure, service-level agreements (SLAs), and compliance practices, which require careful evaluation and ongoing trust.
Thermal Risks and Overheating in Equipment Rooms	**Mitigation** Mitigation is the most effective way to address overheating risks in high-density equipment areas like server rooms and wiring closets. Heat buildup can result from poor ventilation, insufficient cooling, or heavy equipment use. To reduce this risk, organizations can use	**Transference** If internal cooling systems are inadequate or unreliable, the organization can transfer the risk by moving critical infrastructure to a third-party data center with professionally managed climate control. These facilities are designed to maintain safe

	low-cost solutions such as temperature sensors, automated heat alerts, and exhaust fans to improve airflow. Proper equipment arrangement to avoid blocked vents and regular inspections also help detect and resolve issues early. These measures provide a practical and affordable way to prevent heat damage and protect infrastructure.	operating conditions, reducing the organization's heat risk management burden. However, this approach adds hosting costs and requires clear vendor agreements to ensure proper access and uptime commitments.
Theft or Loss of Physical IT Equipment	**Mitigation** Mitigation is the most suitable treatment for theft of IT assets such as laptops, hard drives, or backup tapes. Simple strategies such as physical cable locks, locked cabinets or server racks, and device tethering in public-facing areas can reduce theft risk without significant expense. Establishing strict sign-out procedures and keeping an accurate asset inventory also helps track devices and support recovery or reporting if items go missing. Encrypting data on mobile devices and backup media also ensures that information stays secure even if the equipment is stolen.	**Transference** As an alternative or addition to mitigation, organizations can transfer the financial risks of theft by obtaining cyber insurance or property insurance policies. These policies can cover the cost of stolen equipment and expenses related to data breaches or legal liabilities. While insurance does not stop theft from occurring, it provides financial protection and can be especially useful in settings where complete physical security is difficult to enforce.
Rogue Access Points and Unauthorized Network Devices	**Mitigation** Mitigation is essential for managing the threat of rogue access points. These unauthorized devices pose a serious risk by bypassing network security controls. Even with limited resources, the organization can deploy free or low-cost wireless scanning tools to monitor for unknown signals. Additional steps like turning off unused Ethernet ports and applying MAC address whitelisting help prevent unauthorized network hardware from connecting. These measures help maintain a secure network environment and enable a quick response if suspicious devices are found.	**Avoidance** If the threat is severe and mitigation is not feasible, the organization might choose avoidance by completely removing wireless connectivity and using only wired networks. Although this eliminates the risk of rogue access points, it may not be practical in flexible or mobile work settings that depend on Wi-Fi. Thus, avoidance is best suited for tightly controlled areas like data centers or secure offices with limited wireless requirements.

People-Based Threats		
Threat Item	**Best Approach**	**Alternative Approach**
Insider Threats and Privileged Misuse by Employees	**Mitigation** The best approach is mitigation, as avoiding this risk is impractical due to necessary internal data access. Mitigation involves implementing technical and procedural controls such as regular audits, user behavior monitoring, and strict role-based access controls. Staff training on security best practices also reduces the likelihood of malicious or accidental insider actions.	**Transference** Even though risk mitigation is considered the best practice, transferring the risk would also be a good alternative, as taking cyber insurance will help the organization avoid any financial loss if the mitigation approach fails.
Poor Cyber Hygiene Practices Across Departments	**Mitigation** Implement continuous security awareness training, enforce clear IT usage policies, and deploy endpoint protection solutions across departments. Security representatives in each department can reinforce safe behavior and report anomalies that will be observed. Regular audits can identify and address hygiene gaps among employees.	**Transference** Cyber hygiene risks may be partially transferred by outsourcing IT operations to a managed security provider (MSP) with SLAs on security hygiene. However, full transfer is not realistic as accountability for daily practices still lies with the internal organization members.
Social Engineering and Phishing Exploits	**Mitigation** Mitigation through continuous employee awareness training, simulated phishing campaigns, and implementation of email filtering systems. A multi-factor authentication (MFA) can also reduce credential abuse for privileged accounts even if phishing attack succeeds.	**Transference** As an alternative, the organization may choose to transfer part of the risk by outsourcing email security services or incident handling to a third-party MSSP (Managed Security Service Provider). While this can reduce the internal workload of existing staff and further provide expert response, it depends heavily on vendor reliability and does not eliminate internal exposure to errors done by users.
System Misconfigurations by Internal Users	**Mitigation** Apply configuration baselines, automated compliance checks, and the principle of least privilege to reduce the likelihood of misconfigurations. In addition, the use Infrastructure as Code (IaC) and change management processes to enforce secure settings can help mitigate such threat.	**Acceptance** In low-risk environments or non-critical systems, minor misconfigurations may be accepted but only temporarily with a corresponding periodic monitoring. However, this is not recommended for core and sensitive systems due to potential exploitation.

Delayed or Inconsistent Security Patch Management	**Mitigation** Automate patch deployment where possible, schedule regular maintenance windows, and use vulnerability scanners to prioritize patching based on risk of devices and their users. Include patching in asset lifecycle policies.	**Avoidance** Avoidance could involve retiring systems that require frequent manual patching, though this may be costly. Risk remains in legacy environments, so mitigation remains the most cost-effective and secure method.
Credential Misuse by Third-Party Contractors	**Mitigation** Enforce strong RBAC policies, implement Just-In-Time (JIT) access and recording sesions that involve third-party credentials. Use MFA and proactive monitoring of third-party activity through SIEM tools.	**Transference** Include clauses and negotioations with third-party contracts that transfer liability in case of misuse. However, legal transfer does not eliminate the operational and reputational impact on the organization.
Malware Risks from Third-Party Software	**Mitigation** Implement application whitelisting, check software sources, and perform static and dynamic analysis before live deployment. Implement sandbox environments to carefully test third-party apps and integrate endpoint detection and response (EDR).	**Avoidance** Avoid installing third-party software entirely, but this may limit the productivity and innovation of certain work requirements. Risk avoidance is only advisable in highly controlled environments, but mitigation strategies is still more ideal.
Loss or Misplacement of Sensitive Client Data	**Transference** The best approach for handling misplaced or stolen client tapes is risk transfer. These tapes may contain sensitive data, and their loss can lead to legal consequences under the Australian Privacy Act 1988 and reputational damage. Using third-party storage providers shifts responsibility for managing and securing the tapes, reducing the organization's liability. Alternatively, data breach insurance can cover financial losses but not reputational harm. Avoidance is impractical due to the necessity of client data, and acceptance is too risky. Transferring the risk is the most cost-effective and responsible option.	**Mitigation** The alternative option would be to mitigate the risk; however, as highlighted previously, it would require multiple control securities, including CCTV, physical access controls, logging of those who enter and use client tapes, and enforcing stricter policies regarding handling the tapes. All these control methods would require a lot of human resources to create the policies, train the staff, monitor the CCTV, and check the logs. Instead of simplifying the transfer of risk, it is less stressful for the organization.
Inadequate Role-Based Access Control (RBAC) Implementation	**Mitigation** Design and enforce RBAC policies based on functions of each employee and personnel, with regular access reviews and audits. Integrate RBAC with identity and access management (IAM) systems to reduce overprivileged accounts and unmonitored user acitivites.	**Acceptance** In early-stage or low-risk environments, organizations might accept temporary RBAC gaps with monitoring in place. However, this approach is unsustainable in the long-term and may result to serious compliance risks.

Processes and Procedures Threats		
Threat Item	**Best Approach**	**Alternative Approach**
Lack of Standardized Onboarding and Offboarding Procedures	**Mitigation** Implement formal onboarding and offboarding processes integrated with HR and IT systems to allow for automated account creation and deactivation.	**Transference** Outsourcing HR access management to a third-party provider shifts responsibility but requires the third-party provider to comply with the organisation's policy and to have a well-written contract.
Lack of Cybersecurity Awareness and Training	**Mitigation** Implement mandatory cybersecurity training and awareness campaigns for all departments. Use virtual environments and focus on phishing, social engineering and device safety.	**Acceptance** Humans will always be the weakest link in security. By accepting this risk, evaluating it and monitoring it thoroughly, threats can be managed in the short term.
Absence of Formal Change Control in R&D Projects	**Mitigation** Develop and use a Change Control Policy that requires approval, proper documentation and a high level of traceability for all R&D system changes.	**Avoidance** Pause the R&D until change management procedures have been implemented. This avoids the threat of unapproved changes, but will delay the current projects.
Lack of Routine Privilege Audit and Oversight	**Mitigation** Regularly scheduled privilege audits and automated tools to flag accounts with excessive access rights.	**Transference** Outsource active monitoring and privilege audits through a third party, which can free up resources but will leave the organisation dependent on the services and require strict contracts to protect data and confidentiality.
Weak After-Hours Access and Visitor Management Process	**Mitigation** Enforce a strict after-hours access policy that requires approval, visitors to sign in and out, and RIFD badge systems.	**Avoidance** Completely stop after-hours access except in emergencies. Doing so reduces security risks but can disrupt staff or vendors who lack schedule flexibility.

6.2 Cost-Benefit Analysis of Controls

This section evaluates the financial justification for implementing certain security controls by comparing the potential loss from security incidents with the cost of mitigation. Using key variables such as Asset Value (AV), Exposure Factor (EF), and Annualized Loss Expectancy (ALE), the analysis determines whether each safeguard attempt offers a net benefit. This supports informed decision-making by balancing risk reduction with cost efficiency.

6.2.1 Cost-Benefit Analysis Variables Reference Table

Column Name	Acronym	Formula	Unit	Description	References/ Standards
Asset	n/a	n/a	n/a	Organizational assets of Cyber Sentinel Inc.	n/a
Asset Value	AV	n/a	AUD ($)	Estimated value of the asset (monetary or impact-based).	*See Appendix C*
Exposure Factor	EF	n/a	Percentage (%)	Percentage of asset value lost in a successful incident (This document uses range from 0-1).	NIST, CIS
Single Loss Expectancy	SLE	$SLE = AV \times EF$	AUD ($)	Estimated loss in one incident.	NIST
Annualized Rate of Occurrence	ARO	n/a	Percentage (%)	Frequency of the incident per year (e.g. This document uses 0.3 = once every ~3 years).	Verizon, ACSC, FAIR Institute
Annualized Loss Expectancy (Pre-Control)	ALE (Pre)	$ALE = SLE \times ARO$	AUD ($)	Annual loss estimates before safeguards.	NIST

Annualized Loss Expectancy (Post-Control)	ALE (Post)	*ALE = SLE × ARO × (adjusted)*	AUD ($)	Annual loss estimate after safeguards are implemented.	SANS Institute, NIST
Annual Cost of Safeguard	ACS	n/a	AUD ($)	Annual cost of implementing the safeguard control or mitigation.	IBM, ISACA
Cost-Benefit Score	CBA Score	*CBA = ALE(pre) – ALE(post) – ACS*	AUD ($)	The net benefit or loss of implementing the control (Positive eqauls to good investment).	n/a

6.2.2 Cost-Benefit Analysis for People-Based Assets

ASSET	AV (AUD)	EF (%)	SLE (AUD)	ARO (%)	ALE PRE (AUD)	ALE POST (AUD)	ACS (AUD)	CBA SCORE (AUD)
Chief Executive Officer (CEO)	$400,000.00	0.7	$280,000.00	0.3	$84,000.00	$25,000.00	$15,000.00	$44,000.00
Chief Security Officer (CSO)	$350,000.00	0.6	$210,000.00	0.4	$84,000.00	$28,000.00	$13,000.00	$43,000.00
Chief Information Officer (CIO)	$350,000.00	0.6	$210,000.00	0.4	$84,000.00	$30,000.00	$14,000.00	$40,000.00
Division Head - R&D	$300,000.00	0.5	$150,000.00	0.4	$60,000.00	$18,000.00	$10,000.00	$32,000.00
Division Head - Data Processing	$300,000.00	0.5	$150,000.00	0.4	$60,000.00	$20,000.00	$10,000.00	$30,000.00
Server Team	$300,000.00	0.7	$210,000.00	0.3	$63,000.00	$20,000.00	$14,000.00	$29,000.00

Division Head - Software	$280,000.00	0.5	$140,000.00	0.4	$56,000.00	$20,000.00	$9,000.00	$27,000.00
Director Sales & Product	$250,000.00	0.5	$125,000.00	0.4	$50,000.00	$18,000.00	$9,000.00	$23,000.00
Network Team	$280,000.00	0.6	$168,000.00	0.3	$50,400.00	$18,000.00	$13,000.00	$19,400.00
Desktop Support Team	$200,000.00	0.4	$80,000.00	0.4	$32,000.00	$10,000.00	$7,000.00	$15,000.00
Manager - Finance	$200,000.00	0.4	$80,000.00	0.4	$32,000.00	$12,000.00	$6,000.00	$14,000.00
Manager - Human Resource	$200,000.00	0.4	$80,000.00	0.4	$32,000.00	$12,000.00	$6,000.00	$14,000.00
Director - Back Office	$220,000.00	0.4	$88,000.00	0.4	$35,200.00	$15,000.00	$8,000.00	$12,200.00
Division Head - Service & Tech Support	$260,000.00	0.4	$104,000.00	0.3	$31,200.00	$12,000.00	$7,000.00	$12,200.00
General Staff (Sales, HR, Support, Marketing)	$150,000.00	0.3	$45,000.00	0.6	$27,000.00	$9,000.00	$6,000.00	$12,000.00
Legal Officer	$220,000.00	0.5	$110,000.00	0.2	$22,000.00	$6,000.00	$6,000.00	$10,000.00
Manager - Legal Department	$200,000.00	0.4	$80,000.00	0.3	$24,000.00	$8,000.00	$6,000.00	$10,000.00
Contractors / Vendors	$180,000.00	0.5	$90,000.00	0.3	$27,000.00	$10,000.00	$8,000.00	$9,000.00
Manager - Officer Admin	$180,000.00	0.3	$54,000.00	0.4	$21,600.00	$9,000.00	$5,000.00	$7,600.00
Manager - Building & Mainten-ance	$180,000.00	0.3	$54,000.00	0.3	$16,200.00	$6,000.00	$4,000.00	$6,200.00

6.2.3 Cost-Benefit Analysis for Procedure-Based Assets

ASSET	AV (AUD)	EF (%)	SLE (AUD)	ARO (%)	ALE PRE (AUD)	ALE POST (AUD)	ACS (AUD)	CBA SCORE (AUD)
Disaster Recovery Plan	$600,000.00	0.8	$480,000.00	0.1	$48,000.00	$9,600.00	$11,000.00	$27,400.00
Incident Response Plan	$400,000.00	0.5	$200,000.00	0.2	$40,000.00	$8,000.00	$9,000.00	$23,000.00
RBAC Imple-mentation	$300,000.00	0.7	$210,000.00	0.25	$52,500.00	$10,500.00	$12,000.00	$30,000.00
User Access Proce-dures	$250,000.00	0.6	$150,000.00	0.3	$45,000.00	$9,000.00	$8,000.00	$28,000.00
Password Policies	$200,000.00	0.5	$100,000.00	0.4	$40,000.00	$12,000.00	$6,000.00	$22,000.00

6.2.4 Cost-Benefit Analysis for Data-Based Assets

ASSET	AV (AUD)	EF (%)	SLE (AUD)	ARO (%)	ALE PRE (AUD)	ALE POST (AUD)	ACS (AUD)	CBA SCORE (AUD)
Client PII	$800,000.00	0.8	$640,000.00	0.3	$192,000.00	$38,400.00	$25,000.00	$128,600.00
Financial Records	$500,000.00	0.7	$350,000.00	0.2	$70,000.00	$17,500.00	$18,000.00	$34,500.00
R&D Prototype Data	$700,000.00	0.6	$420,000.00	0.25	$105,000.00	$31,500.00	$20,000.00	$53,500.00
On-Prem File Servers & Backups	$550,000.00	0.6	$330,000.00	0.2	$66,000.00	$16,500.00	$14,000.00	$35,500.00
Data Analysis for Client Projects	$450,000.00	0.6	$270,000.00	0.2	$54,000.00	$13,500.00	$13,000.00	$27,500.00
Cloud Storage	$600,000.00	0.5	$300,000.00	0.3	$90,000.00	$21,000.00	$16,000.00	$53,000.00
Remote Testing of Prototypes	$400,000.00	0.5	$200,000.00	0.3	$60,000.00	$18,000.00	$12,000.00	$30,000.00
Email Comm-unications	$300,000.00	0.4	$120,000.00	0.4	$48,000.00	$14,400.00	$10,000.00	$23,600.00

6.2.5 Cost-Benefit Analysis for Software-Based Assets

ASSET	AV (AUD)	EF (%)	SLE (AUD)	ARO (%)	ALE PRE (AUD)	ALE POST (AUD)	ACS (AUD)	CBA SCORE (AUD)
CRM Software	$500,000.00	0.7	$350,000.00	0.25	$87,500.00	$26,250.00	$15,000.00	$46,250.00
Firewalls	$500,000.00	0.7	$350,000.00	0.2	$70,000.00	$14,000.00	$13,000.00	$43,000.00
Windows Server	$550,000.00	0.6	$330,000.00	0.3	$99,000.00	$29,700.00	$18,000.00	$51,300.00
IDS/IPS Systems	$450,000.00	0.6	$270,000.00	0.25	$67,500.00	$20,250.00	$11,000.00	$36,250.00
Email Systems	$400,000.00	0.6	$240,000.00	0.3	$72,000.00	$21,600.00	$12,000.00	$38,400.00
Anti-Virus Software	$350,000.00	0.6	$210,000.00	0.3	$63,000.00	$18,900.00	$10,000.00	$34,100.00
SIEM Tools	$600,000.00	0.5	$300,000.00	0.2	$60,000.00	$15,000.00	$20,000.00	$25,000.00
Linux VM	$300,000.00	0.5	$150,000.00	0.2	$30,000.00	$9,000.00	$7,000.00	$14,000.00
macOS Systems	$250,000.00	0.4	$100,000.00	0.1	$10,000.00	$4,000.00	$4,000.00	$2,000.00

6.2.6 Cost-Benefit Analysis for Hardware-Based Assets

ASSET	AV (AUD)	EF (%)	SLE (AUD)	ARO (%)	ALE PRE (AUD)	ALE POST (AUD)	ACS (AUD)	CBA SCORE (AUD)
Servers	$800,000.00	0.8	$640,000.00	0.2	$128,000.00	$32,000.00	$20,000.00	$76,000.00
Laptops	$300,000.00	0.7	$210,000.00	0.3	$63,000.00	$18,900.00	$10,000.00	$34,100.00
Desktops	$200,000.00	0.5	$100,000.00	0.2	$20,000.00	$6,000.00	$5,000.00	$9,000.00
USB Devices	$150,000.00	0.6	$90,000.00	0.4	$36,000.00	$10,800.00	$7,000.00	$18,200.00
CCTV Cameras	$120,000.00	0.4	$48,000.00	0.2	$9,600.00	$2,400.00	$6,000.00	$1,200.00
Biometric Scanners	$100,000.00	0.5	$50,000.00	0.15	$7,500.00	$2,500.00	$4,000.00	$1,000.00

6.2.7 Cost-Benefit Analysis for Networking-Based Assets

ASSET	AV (AUD)	EF (%)	SLE (AUD)	ARO (%)	ALE PRE (AUD)	ALE POST (AUD)	ACS (AUD)	CBA SCORE (AUD)
SaaS Platforms	$600,000.00	0.6	$360,000.00	0.2	$72,000.00	$21,600.00	$18,000.00	$32,400.00
VPN	$550,000.00	0.7	$385,000.00	0.2	$77,000.00	$23,100.00	$15,000.00	$38,900.00
Internal Web Portals	$500,000.00	0.6	$300,000.00	0.2	$60,000.00	$18,000.00	$14,000.00	$28,000.00
Cloud Backup Services	$500,000.00	0.5	$250,000.00	0.2	$50,000.00	$15,000.00	$12,000.00	$23,000.00
File Shares	$450,000.00	0.6	$270,000.00	0.25	$67,500.00	$20,250.00	$11,000.00	$36,250.00
Routers	$400,000.00	0.6	$240,000.00	0.25	$60,000.00	$18,000.00	$12,000.00	$30,000.00
Remote Access Tools	$400,000.00	0.6	$240,000.00	0.3	$72,000.00	$21,600.00	$13,000.00	$37,400.00
Switches	$300,000.00	0.5	$150,000.00	0.2	$30,000.00	$9,000.00	$7,000.00	$14,000.00
Wireless Access Points	$250,000.00	0.7	$175,000.00	0.3	$52,500.00	$15,750.00	$10,000.00	$26,750.00

References

Aamir, M., Ahmed Kalwar, K., & Mekhilef, S. (2016). Review: Uninterruptible Power Supply (UPS) system. Renewable & Sustainable Energy Reviews, 58, 1395–1410. https://doi.org/10.1016/j.rser.2015.12.335

About PSPF. (n.d.). Protective Security Policy Framework. https://www.protectivesecurity.gov.au/about

Australian Cyber Security Centre. (2023). Essential Eight Maturity Model. https://www.cyber.gov.au

Australian Cyber Security Centre. (2024). ACSC Annual cyber threat report: July 2022 to June 2023. https://www.cyber.gov.au/threats

Australian Government. (1968). Copyright Act 1968 (Cth). https://www.legislation.gov.au/C1968A00063/latest/text

Australian Government. (1988). Privacy Act 1988 (Cth). Office of the Australian Information Commissioner. https://www.oaic.gov.au/privacy-law/privacy-act

Australian Government. (n.d.). Corporations Act 2001. Federal Register of Legislation. Retrieved from https://www.legislation.gov.au/Series/C2004A00818

Australian Government. (n.d.). Notifiable Data Breaches scheme. Office of the Australian Information Commissioner. Retrieved from https://www.oaic.gov.au/privacy/notifiable-data-breaches

Australian Government. (n.d.). Privacy Act 1988. Office of the Australian Information Commissioner. Retrieved from https://www.legislation.gov.au/C2004A03712/latest/textChange management policy. (2020). https://www.doa.la.gov/media/lhibcody/ots_change_management_policy.pdf

Australian Government. (n.d.). Protective Security Policy Framework (PSPF). Attorney-General's Department. Retrieved from https://www.protectivesecurity.gov.au

Australian Government. (n.d.). Telecommunications (Interception and Access) Act 1979. Department of Home Affairs. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/telecommunications-interception-and-surveillance:contentReference[oaicite:5]{index=5}

Australian Government. (n.d.). Work Health and Safety Act 2011. Federal Register of Legislation. Retrieved from https://www.legislation.gov.au/Details/C2011A00137

Australian Signals Directorate. (n.d.). Essential Eight. Cyber.gov.au. https://www.cyber.gov.au/acsc/view-all-content/essential-eight:contentReference[oaicite:2]{index=2}

Björkman, K., Holmberg, J.-E., & Mätäsniemi, T. (2022). Comparing physical protection strategies against insider threats using probabilistic risk assessment. Nuclear Engineering and Design, 391, 111738-. https://doi.org/10.1016/j.nucengdes.2022.111738

Breachsense. (2024, December 8). Equifax data breach case study. BreachSense. https://www.breachsense.com/blog/equifax-data-breach/

Britannica. (n.d.). Information system. Retrieved from https://www.britannica.com/topic/information-system

Calder, A. (2023). ISO 27001/ISO 27002: A guide to information security management systems (1st ed.). IT Governance Publishing. https://doi.org/10.2307/jj.9039966

Capital One. (n.d.). 2019 Capital One cyber incident: What happened. https://www.capitalone.com/digital/facts2019/

Center for Internet Security. (n.d.). CIS risk assessment methodology. https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method

Clinton, Larry. Cybersecurity for Business: Organization-Wide Strategies to Ensure Cyber Risk Is Not Just an IT Issue. London: Kogan Page Limited, 2022.

Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man In The Middle Attacks. IEEE Communications Surveys and Tutorials, 18(3), 2027–2051. https://doi.org/10.1109/COMST.2016.2548426

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027–2051. https://doi.org/10.1109/COMST.2016.2548426

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). Understanding and Responding to Distributed Denial-of-Service Attacks. Retrieved from https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf

Delinea. (n.d.). Cybersecurity Incident Response Plan Template. https://delinea.com/resources/free-incident-response-plan-template

Deng, Q., Pu, J., Tan, Z., Qian, Z., & Krishnamurthy, S. (n.d.). Beyond the Horizon: Uncovering Hosts and Services Behind Misconfigured Firewalls. https://www.cs.ucr.edu/~zhiyunq/pub/oakland25_firewall_misconfig.pdf

Dietrich, C., Krombholz, K., Borgolte, K., & Fiebig, T. (2018). Investigating System Operators' Perspective on Security Misconfigurations. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3243734.3243794

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2021). Software security patch management—A systematic literature review of challenges, approaches, tools, and practices. Information and Software Technology, 144(0950-5849), 106771. https://doi.org/10.1016/j.infsof.2021.106771

EPIC - Spotlight on Surveillance - May 2006. (n.d.). https://archive.epic.org/privacy/surveillance/spotlight/0506/default.html

European Parliament & Council of the European Union. (2016, April 27). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

FAIR Institute. (n.d.). Factor Analysis of Information Risk (FAIR). https://www.fairinstitute.org

Federal Register of Legislation. (n.d.). https://www.legislation.gov.au/

Fottrell, S. M. (2025, February). Information security vs. cybersecurity: What's the difference? Forbes Advisor. https://www.forbes.com/advisor/education/it-and-tech/information-security-vs-cybersecurity/

Gartner. (2023). IT key metrics data: Infrastructure and operations. https://www.gartner.com

Gibraltarsoultions. (2024, August 20). 10 Critical IT Policies for Every Organization. Gibraltarsolutions.com. https://gibraltarsolutions.com/blog/10-critical-it-policies-for-every-organization/

Glassdoor. (n.d.). Salaries in Australia. https://www.glassdoor.com.au

Grimes, R. A. (2024). Fighting Phishing : Everything You Can Do to Fight Social Engineering and Phishing. (1st ed.). John Wiley & Sons, Incorporated.

Haletky, E. (2009). VMware vSphere and virtual infrastructure security : securing the virtual environment (1st edition). Prentice Hall.

IBM Security. (2024). Cost of a data breach report 2024. https://www.ibm.com/security/data-breach

International Organization for Standardization. (2022). ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks (4th ed.). https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en

ISACA. (2019). COBIT 2019 framework: Governance and management objectives. https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf

ISO/IEC. (2016). ISO/IEC 27004:2016 – Information security management – Monitoring, measurement, analysis and evaluation. International Organization for Standardization.

Jero, S., Furgala, J., Pan, R., Gadepalli, P. K., Clifford, A., Ye, B., Khazan, R., Ward, B. C., Parmer, G., & Skowyra, R. (2021). Practical Principle of Least Privilege for Secure Embedded Systems. 2021 IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS). https://doi.org/10.1109/rtas52030.2021.00009

Kamerer, Jessica L, and Donna S McDermott. “Cyber Hygiene Concepts for Nursing Education.” Nurse Education Today 130 (2023): 105940–105940. https://doi.org/10.1016/j.nedt.2023.105940.Alicea, M., & Alsmadi, I. (2021). Misconfiguration in Firewalls and Network Access Controls: Literature Review. ProQuest, 13(11), 283. https://doi.org/10.3390/fi13110283

Karen Scarfone (NIST), Wayne Jansen (NIST), & Miles Tracy (Federal Reserve Information Technology). (2008). Guide to general server security. NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/pubs/sp/800/123/final

Kaseya VSA Supply-Chain Ransomware Attack | CISA. (2021, July 2). Www.cisa.gov. https://www.cisa.gov/news-events/alerts/2021/07/02/kaseya-vsa-supply-chain-ransomware-attack

Kerr, D., Gammack, J., & Boddington, R. (2011). Overview of digital business security issues. In D. Kerr, J. Gammack, & K. Bryant (Eds.), Overview of digital business security issues (pp. 1–36). IGI Global.

Krebs, B. (2014, February 5). Target Hackers Broke in Via HVAC Company — Krebs on Security. Krebsonsecurity.com. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Lanz, J. (2024). Addressing Patch Management Risk: EBSCOhost. Retrieved June 6, 2025, from Ebscohost.com website: https://web.p.ebscohost.com/ehost/detail/detail?vid=0&sid=89b4a61f-20db-46a7-9b95-dcd4d148d8a3%40redis&bdata=JkF1dGhUeXBlPXNoaWImc2l0ZT1laG9zdC1saXZl#AN=182334422&db=bsu

Lasky, S. (2022). Tailgating Has Evolved Into a Top Security Priority. In Security technology & design (Vol. 32, Number 4, pp. 32–34). Endeavor Business Media.

Lee, D. (2019). A thief stole unencrypted hard drives filled with 29,000 Facebook employees' information. The Verge. https://www.theverge.com/2019/12/13/21020736/facebook-theft-unencrypted-drives-employee-payroll-security

Lemos, R. (2016). How to keep USB thumbdrive malware away from your PC. In PC world (Vol. 34, Number 7, pp. 146-). IDG Consumer & SMB, Inc.

Lensu, Vladimir (2013). Building Secure IT Server Room. https://urn.fi/URN:NBN:fi:amk-2013052811228

Libeer, L. (2024, October 18). Rogue Device Detection: Preventing vulnerabilities and threats. Lansweeper. https://www.lansweeper.com/blog/cybersecurity/rogue-device-detection-preventing-vulnerabilities-and-threats/

Lindemulder, G., & Kosinski, M. (2024, June 11). What is a man-in-the-middle (MITM) attack? IBM. https://www.ibm.com/think/topics/man-in-the-middle

M. Anedda, Floris, A., R. Girau, M. Fadda, P. Ruiu, Farina, M., A. Bonu, & Giusto, D. (2023). Privacy and Security Best Practices for IoT Solutions. IEEE Access, 11, 129156–129172. https://doi.org/10.1109/access.2023.3331820

Marvin, M. (2023, November 3). Beware the dangers of the rogue access point. Portnox. https://www.portnox.com/blog/cyber-attacks/beware-the-dangers-of-the-rogue-access-point

Matthew Prince. (2023, November 4). Post mortem on the Cloudflare control plane and analytics outage. The Cloudflare Blog. https://blog.cloudflare.com/post-mortem-on-cloudflare-control-plane-and-analytics-outage/

Mccreight, T., & Leece, D. (2016). Physical security and IT convergence: Managing the cyber-related risks. Journal of Business Continuity & Emergency Planning, 10(1), 18–30. https://doi.org/10.69554/PGJO8341

Mohammad Hasan Sadeghi Moghadam, & Seyeed Mohammad Tabatabai Nejad. (2012). A Concise Review of Non-Disclosure Agreement A Concise Review of Non-Disclosure Agreement. Faṣlnāmah-i pizhūhish-i ḥuqūq-i khuṣūṣī, 1(2), 89–115.

Mohan, K., Xu, P., Cao, L., & Ramesh, B. (2008). Improving change management in software development: Integrating traceability and software configuration management. Decision Support Systems, 45(4), 922–936. https://doi.org/10.1016/j.dss.2008.03.003

Nada, S. A., Said, M. A., & Rady, M. A. (2016). CFD investigations of data centers' thermal performance for different configurations of CRACs units and aisles separation. Alexandria Engineering Journal, 55(2), 959–971. https://doi.org/10.1016/j.aej.2016.02.025

NASDAQ OMX Corporate Solutions. (2021). OneLogin automates advanced identity lifecycle management processes, provides "any-to-any" connectivity with robust integrations: New offerings streamline workflows and reduce security risks for onboarding and offboarding. NASDAQ OMX's News Release Distribution Channel.

Nath Nayak, G., Ghosh Samaddar, S., Hang, Y., Desheng, W., & Sandhu, P. (2010). Different flavours of Man-In-The-Middle attack, consequences and feasible solutions. 2010 3rd International Conference on Computer Science and Information Technology, 5, 491–495. https://doi.org/10.1109/ICCSIT.2010.5563900

National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (NIST SP 800-30 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2025, March). Computer security. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/computer_security

National Institute of Standards and Technology. (2025, March). Information security. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/information_security

NCSC. (2025). Denial of service (Dos) guidance. https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection#:~:text=A%20denial%20of%20service%20(DoS)%20attack%20is,money%20to%20analyse%2C%20defend%20and%20recover%20from

Nicholson, P. (2023). Five most famous DDoS attacks and then some. A10 Networks. https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

Nurse, J.R.C. et al. (2014). A Critical Reflection on the Threat from Human Insiders – Its Nature, Industry Perceptions, and Detection Approaches. In: Tryfonas, T., Askoxylakis, I. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2014. Lecture Notes in Computer Science, vol 8533. Springer, Cham. https://doi.org/10.1007/978-3-319-07620-1_24

Office of the Australian Information Commissioner. (2023, March 10). Privacy regulations. OAIC. https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/privacy-regulations

Office of the Australian Information Commissioner. (2024, December 10). The Privacy Act. OAIC. https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act

Office of the Australian Information Commissioner. (2024). About the Notifiable Data Breaches scheme. OAIC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme

PayScale. (n.d.). Australia salary data. https://www.payscale.com/research/AU/Country=Australia

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC press.

Pioneering New TetraGate(TM) Eliminates “Tailgating” as Security Risk at Building Access Points; Breakthrough Software, Developed and Owned by epcSolutions, Is at Center of Gen2 EPC/RFID and Biometric Facial Recognition Solution for Advanced Checkpoint Security. (2006). In PR Newswire. PR Newswire Association LLC.

Provos, N., Friedl, M., & Honeyman, P. (2003). 12th USENIX Security Symposium — Technical Paper. Www.usenix.org. https://www.usenix.org/legacy/event/sec03/tech/full_papers/provos_et_al/provos_et_al_html/

Risk Assessment & Business Continuity Planning | Roles & risks. (2024, May 16). CPD Online College. https://cpdonline.co.uk/knowledge-base/business/risk-assessment-business-continuity-planning

Ritchey, D. (2019). Tailgating: A Common Courtesy and a Common Risk. Security, 56(9), 52–55.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Jeimy J. Cano M. (2019). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. Journal of Cases on Information Technology, 21(3), 26–39. https://doi.org/10.4018/JCIT.2019070102

Salem, Mostafa Aboulnour, and Abu Elnasr E Sobaih. “A Quadruple ‘E’ Approach for Effective Cyber-Hygiene Behaviour and Attitude toward Online Learning among Higher-Education Students in Saudi Arabia amid COVID-19 Pandemic.” Electronics (Basel) 12, no. 10 (2023): 2268-. https://doi.org/10.3390/electronics12102268.

Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. IEEE Communications Magazine, 32(9), 40–48. https://doi.org/10.1109/35.312842

SANS Institute. (n.d.). Risk assessment and mitigation best practices. https://www.sans.org/white-papers

Sarpong Adu-Manu, K., Kwasi Ahiable, R., Kwame Appati, J., & Essel Mensah, E. (2022). Phishing Attacks in Social Engineering: A Review. Journal of Cyber Security (Henderson, Nev.), 4(4), 239–267. https://doi.org/10.32604/jcs.2023.041095

Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS) (Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

Sumo Logic. (n.d.). Information security management. https://www.sumologic.com/glossary/information-security-management

The 20. (2025). The cost of IT downtime. https://www.the20.com/blog/the-cost-of-it-downtime/

Tripwire. (2020). Consequences of non-compliance: Cybersecurity risks and penalties. State of Security. https://www.tripwire.com/state-of-security/consequences-non-compliance-cybersecurity-risks-and-penalties

University of New England. (n.d.). https://compliance.une.edu.au/directory/summary.php?legislation=536

Verizon. (2024). 2024 data breach investigations report. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Vishwanath, Arun, Loo Seng Neo, Pamela Goh, Seyoung Lee, Majeed Khader, Gabriel Ong, and Jeffery Chin. “Cyber Hygiene: The Concept, Its Measure, and Its Initial Tests.” Decision Support Systems 128 (2020): 113160-. https://doi.org/10.1016/j.dss.2019.113160.

Walters, R. (2023). Illegal Interception of Data. In Cybersecurity and Data Laws of the Commonwealth (pp. 267–274). Springer. https://doi.org/10.1007/978-981-99-3935-0_17

Wang, X., Wang, X., Xing, G., Chen, J., Lin, C.-X., & Chen, Y. (2013). Intelligent Sensor Placement for Hot Server Detection in Data Centers. IEEE Transactions on Parallel and Distributed Systems, 24(8), 1577–1588. https://doi.org/10.1109/TPDS.2012.254

What is a Rogue Access Point? How It Works & Examples | Twingate. (n.d.). https://www.twingate.com/blog/glossary/rogue%20access%20point

Whitman, M., & Mattord, H. (2018). Management of information security (Sixth edition). Cengage Learning.

Whitty, M. T., Ruddy, C., Keatley, D., Butavicius, M., & Grobler, M. (2024). The prince of insiders: a multiple pathway approach to understanding IP theft insider attacks. Information and Computer Security, 14. https://doi.org/10.1108/ICS-11-2023-0210

Wisnubroto, D. S., Khairul, K., Basuki, F., & Kristuti, E. (2023). Preventing and countering insider threats and radicalism in an Indonesian research reactor: Development of a human reliability program (HRP). Heliyon, 9(5), e15685–e15685. https://doi.org/10.1016/j.heliyon.2023.e15685

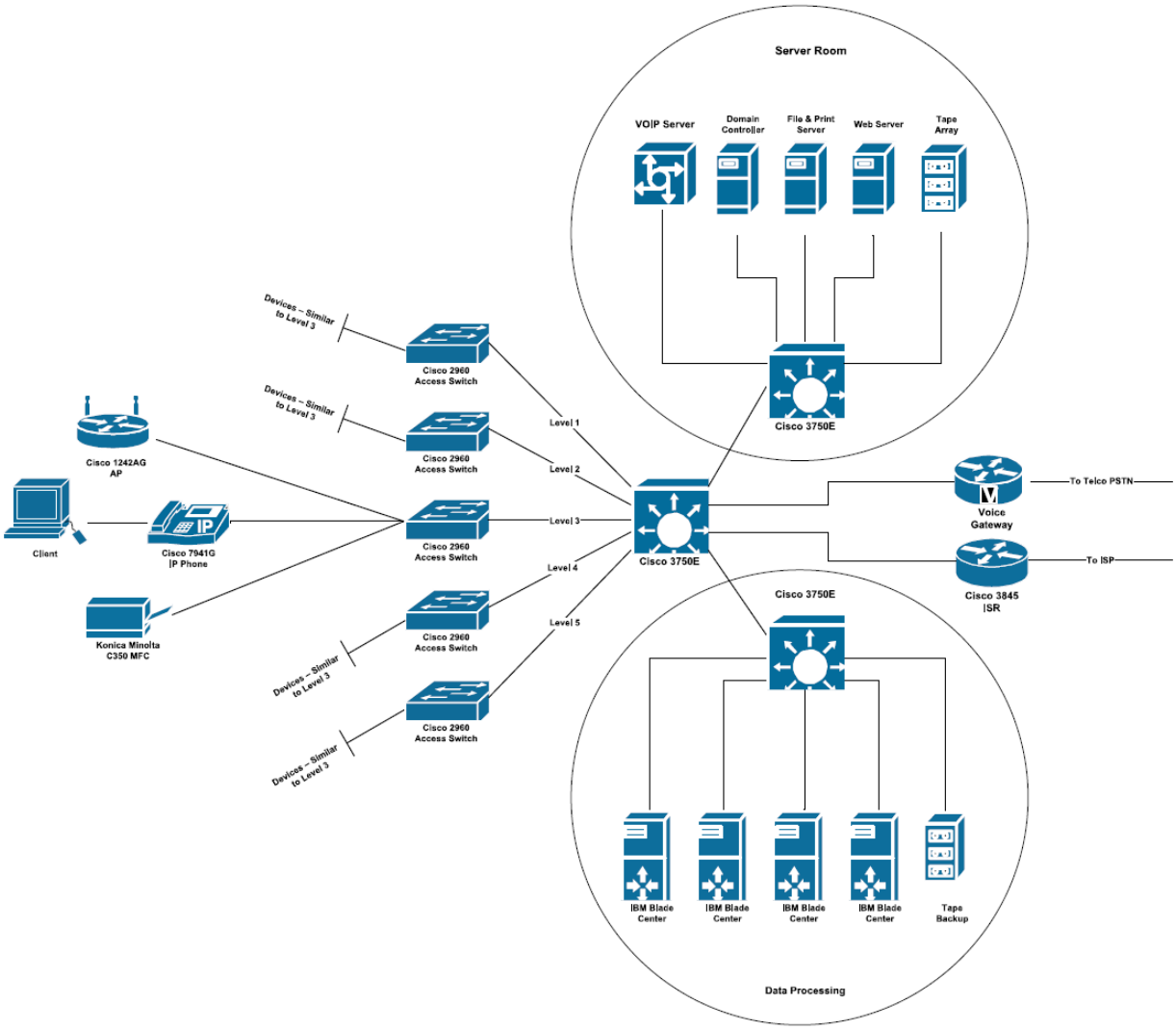
Xu, Z., Wang, H., Xu, Z., & Wang, X. (2014). Power attack: An increasing threat to data centers. Proceedings of the Network and Distributed System Security Symposium (NDSS). https://doi.org/10.14722/ndss.2014.23235

Zeng, D., Su, P. P., Madan, R., & Wang, Y. (2021). Evaluation of flammability and smoke corrosivity of data/power cables used in data centers. Fire Safety Journal, 120, 103094-. https://doi.org/10.1016/j.firesaf.2020.103094

Appendix

Appendix A

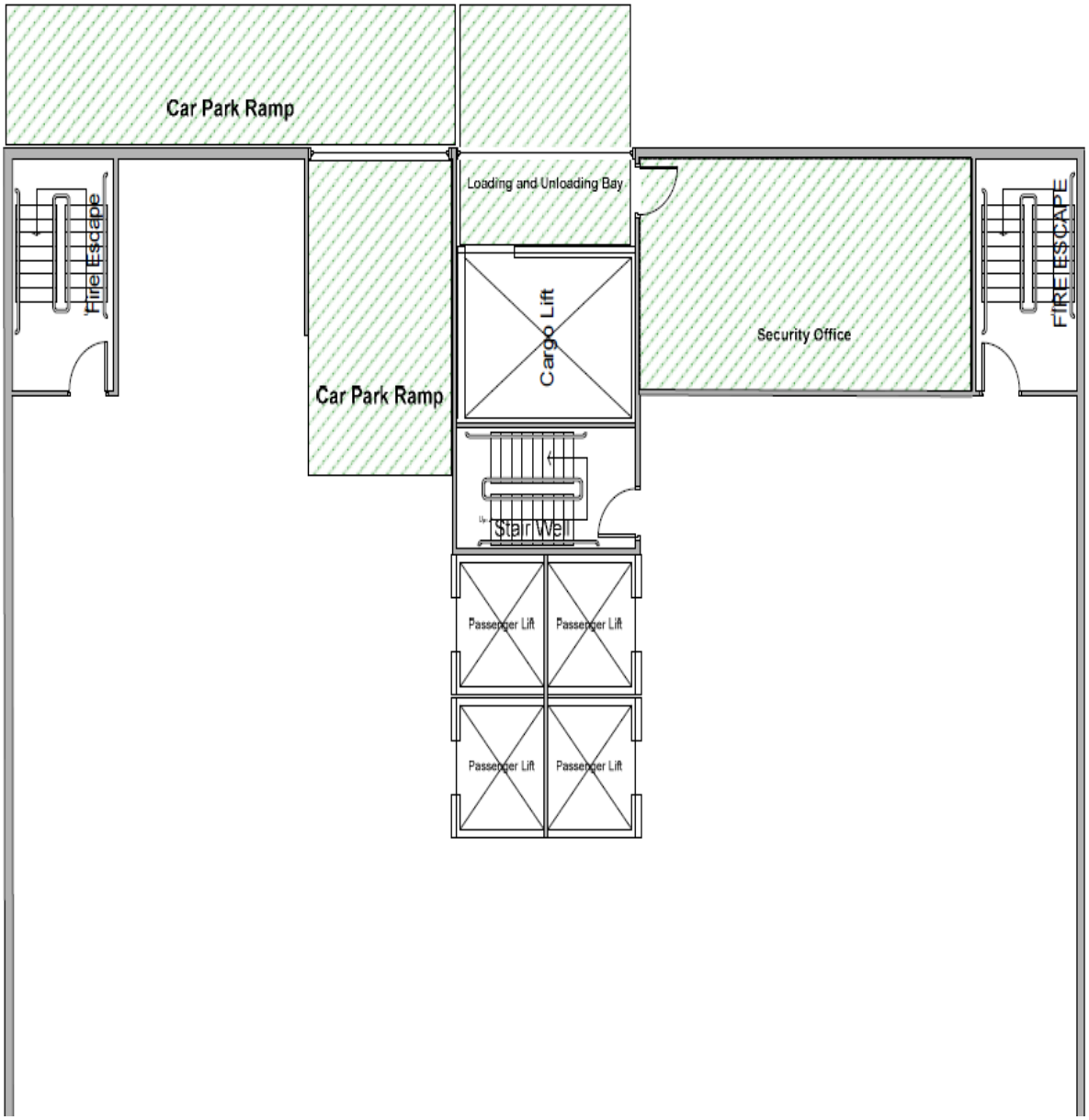
NETWORK INFRASTRUCTURE



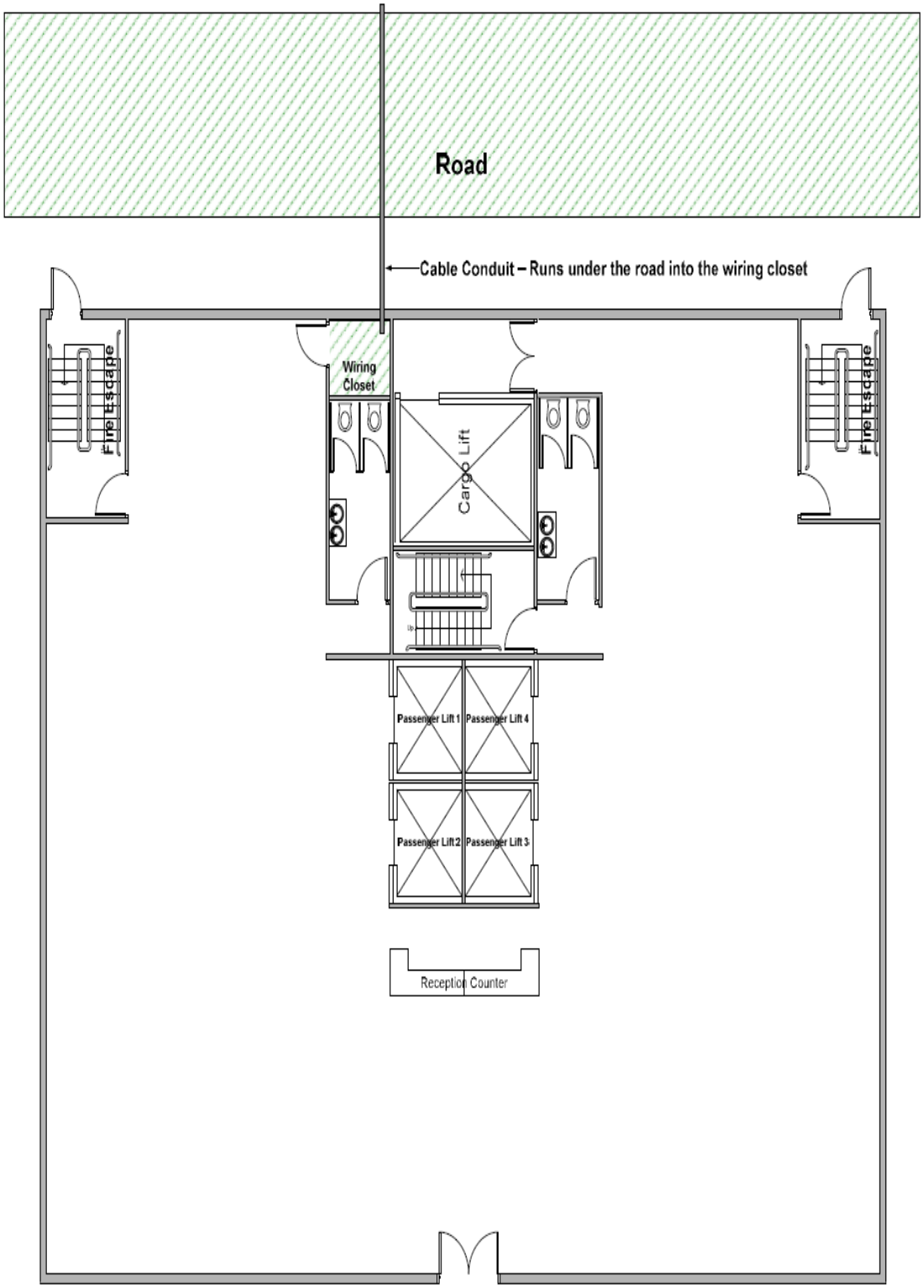
Appendix B

FLOOR PLANS

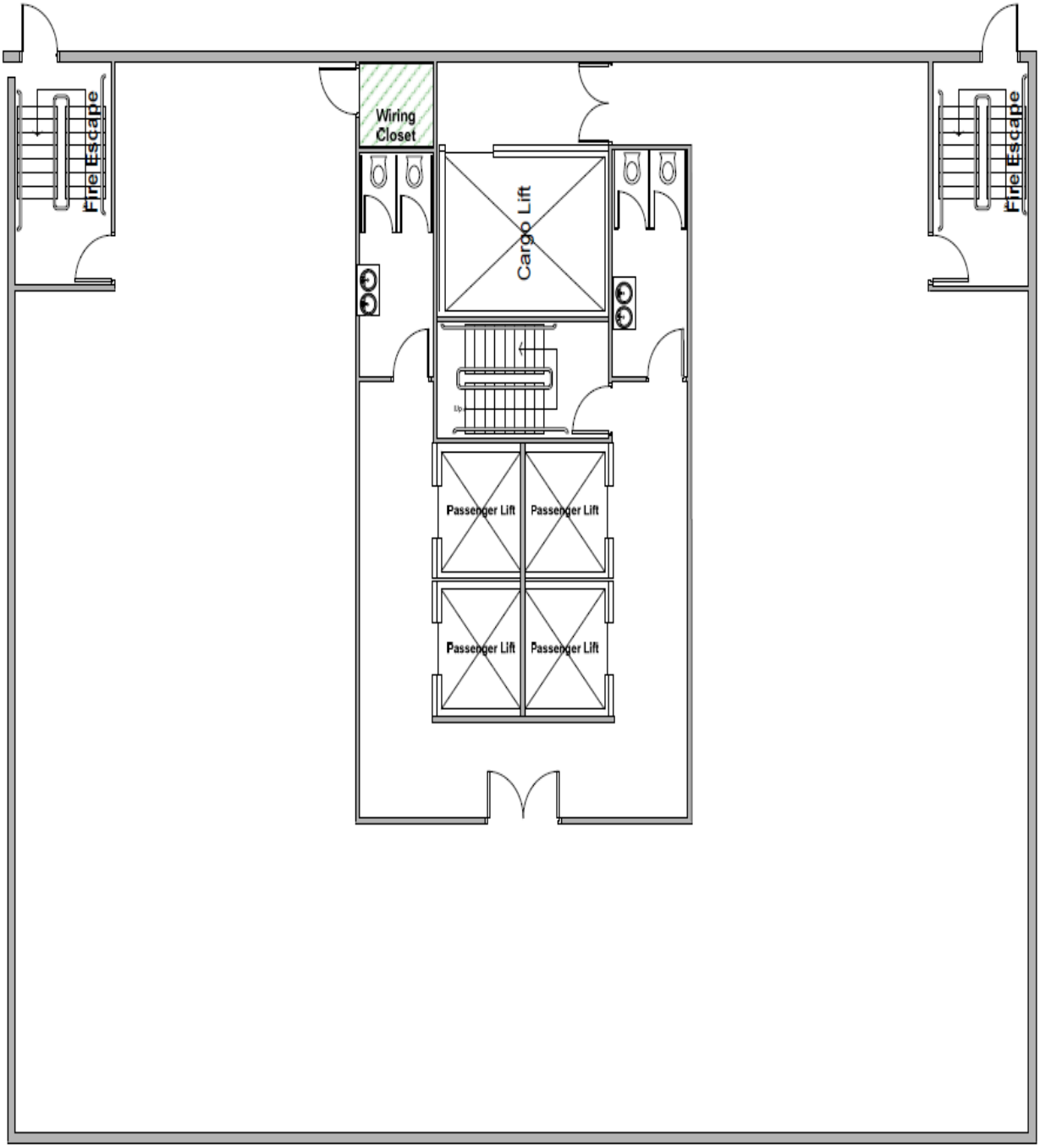
A. Floor Plan – Basement Level



B. Floor Plan – Ground Level



C. Floor Plan – Upper Levels



Appendix C

JUSTIFICATION TABLE FOR ASSET VALUES

Category	Value Range	Justification Summary	References/ Standards
People	$150,000 to $400,000	Values reflect: • employee seniority, • decision-making responsibility, • access to critical systems, • potential legal/operational impact if compromised CEO/CSO/CIO lead governance, while general staff have less exposure risk.	Based on current rates of Cyber Sentinel Inc. and market salaries (Glassdoor, Payscale AU) • NIST SP 800-30 (risk impact based on role exposure) • ISO/IEC 27005 (asset classification by importance)
Procedures	$200,000 to $600,000	AV reflects the procedure's role in: • supporting business continuity, • legal compliance, • security posture DRP and IRP are most critical due to uptime impact and incident handling.	• ISO/IEC 27001 Annex A (A.17: continuity) • NIST SP 800-34 Rev. 1 (Contingency Planning) • ACSC Essential Eight
Data	$300,000 to $800,000	High values due to: • sensitivity (e.g., PII), • proprietary nature (R&D), • legal exposure (privacy breaches), • operational dependence Client PII is most valuable due to legal implications.	• Australian Privacy Act 1988, NDB Scheme • ISO/IEC 27005 (information asset value)
Software	$250,000 to $600,000	AV reflects: • criticality to detection (e.g., SIEM), • business functions (CRM, email), • endpoint protection Systems with compliance impact or integration complexity have higher values.	• NIST SP 800-53 (control families) • Verizon DBIR (2023)
Hardware	$100,000 to $800,000	AV determined by: • replacement cost, • operational role, • data storage risk Servers carry highest risk due to hosting business-critical data and services.	• ISO/IEC 27005 (physical asset classification)
Networking	$250,000 to $600,000	AV reflects: • function in uptime, • remote access, • data availability SaaS, VPN, and portals hold high AV due to business continuity dependency and user interface exposure.	• NIST SP 800-115 (network testing) • ISO/IEC 27033 (network security) • ACSC Threat Report (2024)

Appendix D

INCIDENT RESPONSE PLAN

Cyber Incident	CIA Category	Privileged Account Breach	Business Impact	Risk Level
A senior manager opens a disguised phishing email on the topic of "urgent IT update". The personnel voluntarily enter credentials on a fake login page believing the email was legitimate. The email sender (attacker) gains internal VPN access and downloads sensitive R&D documents.	Confidentiality Compromised Integrity Potentially Affected Availability Not Directly Affected	Yes The identified method of breaching is phishing, requesting credential verification	Severe Notable imapcts highlighted are: • Financial loss • Reputational damage • Operational disruption	High

Actions Taken During Incident Response

To demonstrate and improve the effectiveness of Cyber Sentinel Inc. incident response team and security tools, Cyber Sentinel Inc. requires a record of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, memory dumps, audits, network traffic, and disk images.

Below is the reporting checklist to use when documenting actions taken to combat a high-level privileged account attack. At Cyber Sentinel Inc., it is our goal to meet compliance requirements and prioritize business continuity to minimize impact and cost.

Phase of Cyber Incident	Action	Team Member/ System	Day/Time Action Taken
Incident Discovery and Confirmation	Describe how the team first learned of the attack (security researcher, partner, customer, auditor, internal security alert, etc.)	Server team	28 May 2025 10:00 am
	Analyze audit logs to identify unusual or suspicious account behavior that indicates a likely attack and confirm an attack has occurred.	Desktop Support team	28 May 2025 11:00 am
	Describe potential attackers, including known or expected capabilities, behaviors, and motivations.	Mr. Damon Duffy, Chief Security Officer	28 May 2025 11:15 am
	Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party.	Desktop Support team	28 May 2025 11:30 am
	Prepare an incident timeline to keep in ongoing record of when the attack occurred and subsequent milestones in analysis and response.	Mr. Bhargav Raj Dutta, Chief Information Technology Officer	28 May 2025 12 pm
	Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites.	Desktop Support Team	28 May 2025 12:30pm
	Evaluate the extent of damage upon discovery and risk to systems and privileged accounts in particular. Audit which privileged accounts have	Server team	29 May 2025 9 am

Incident Discovery and Confirmation	been used recently, whether any passwords have been changed, and what applications have been executed.		
	Review your information assets list to identify which assets have been potentially compromised. Note integrity of assets and evidence gathered.	Software team	29 May 2025 9:30 am
	Diagram the path of the incident/attack to provide an “at-a-glance” view from the initial breach to escalation and movement tracked across the network	R&D team	29 May 2025 10 am
	Collect meeting notes in a central repository to use in preparing communications with stakeholders	Mr. Bhargav Raj Dutta, Chief Information Technology Officer	29 May 2025 10:45
	Inform employees regarding discovery.	Mr. Bhargav Raj Dutta, Chief Information Technology Officer	29 May 2025 11:00 am
	Analyze incident Indicators of Compromise with threat intelligence tools	Mr. Damon Duffy, Chief Security Officer	29 May 2025 12:00 pm
	Share information externally about breach of discovery. You may choose to hold communications during this phase until you have contained the breach in order to increase your chances of catching the attacker. If so, make sure that it aligns with your compliance requirements.	Bhargav Raj Dutta (Legal Matter)	29 May 2025 1 pm

Containment and Continuity	Enable temporary privileged accounts to be used by the technical and security team to quickly access and monitor systems.	Mr. Bhargav Raj Dutta, Chief Information Technology Officer	June 8 2025 9 am
	Protect evidence. Back up any compromised systems as soon as possible, prior to performing any actions that could affect data integrity on the original media.	Server Team	June 8 2025 10 am
	Force multi-factor authentication or peer review to ensure privileges are being used appropriately.	Mr. Damon Duffy, Chief Security Officer	June 8 2025 11 am
	Change passwords for all users, service, application, and network accounts.	Network Team	June 8 2025 1 pm
	Increase the sensitivity of application security controls (allowing, denying, and restricting) to prevent malicious malware from being distributed by the attacker.	Network Team	June 8 2025 2 pm
	Remove systems from production or take systems offline if needed.	Desktop team	June 8 2025 3 pm
	Inform employees regarding breach containment.	HR Team	June 14 2025 9 AM
	Analyze, record and confirm any instances of potential data exfiltration occurrences across the network	Server Team	June14 2025 10 am
	Share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.)	Bhargav Raj Dutta (Legal Matter)	June 14 2025 12 pm

Eradication	Close firewall ports and network connections.	Network Team	10 July 2025 8 am
	Test devices and applications to be sure any malicious code is removed.	Server Team	10 July 2025 9 am
	Compare data before and after the incident to ensure systems are reset properly.	Data Processing Team	10 July 2025 10 am
	Inform employees regarding eradication.	HR Team	10 July 2025 10:30 am
	Share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.)	Mr. Bhargav Raj Dutta, Chief Information Technology Officer	10 July 2025 12 pm
Recovery	Download and apply security patches.	Server Team	July 12 2025 9:30 am
	Close network access and reset passwords.	Network Team	July 12 2025 10:12 am
	Conduct vulnerability analysis.	Mr. Damon Duffy, Chief Security Officer	July 12 2025 10:30 am
	Return any systems that were taken offline to production.	Desktop Team	July 12 2025 11 am
	Inform employees regarding recovery.	Ms. Klaryss Puno, Chief Executive Officer and HR	July 12 2025 12 pm
	Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.)	Ms. Klaryss Puno, Chief Executive Officer and HR	July 12 2025 4 pm

Lessons Learned	Review forensic evidence collected.	Server and Security Team	July 14 2025 10 am
	Assess incident costs.	Mr. Bhargav Raj Dutta, Chief Information Technology Officer, Finance Manager	July 14 2025 11 am
	Write an Executive Summary of the incident	Mr. Bhargav Raj Dutta, Chief Information Technology Officer	July 14 2025 12 pm
	Report to the executive team and auditors if necessary.	Server Team	July 14 2025 1 pm
	Implement additional training for everyone involved in incident response and all employees.	Training and Support Team	July 14 2025 2 pm
	Update the incident response plan.	Mr. Damon Duffy, Chief Security Officer	July 15 2025 10 am
	Inform employees regarding lessons learned, additional training, etc.	Ms. Klaryss Puno, Chief Executive Officer, Mr. Damon Duffy, Chief Security Officer, HR	July 15 2025 12 pm
	Share information externally (website updates, emails, social media posts, tech support bulletins, etc.)	Legal office and Ms. Klaryss Puno, Chief Executive Officer	July 15 2025 4 pm

Incident Response Phases

Incident Response Phase	Incident Response Actions Supported by Cyber Sentinel Inc.
Incident Discovery and Confirmation	• Unusual activity was detected from privileged accounts through anomaly detection tools. • Alerts are triggered for multiple failed login attempts and access from distant locations. • Escalated the incident and initiated an immediate investigation. • Review security logs, user activity reports, and network traffic to confirm staff credential compromise. • Consult threat intelligence feeds for known indicators of compromise (IOCs). • Develop an incident timeline to track key activities and identify the cause of the compromise.
Containment and Continuity	• Lock all the affected privileged accounts to prevent continued unauthorized access. • Conduct emergency password resets for the affected accounts. • Enforce Multi-Factor Authentication (MFA) on all administrative accounts. • Update firewall rules to block the suspicious traffic and malicious IP addresses. • Limit access to critical systems to only essential personnel to keep them running. • Secure backups of key systems and data help recover and preserve evidence.
Eradication	• Remove all malware, unauthorised scripts and backdoors found during forensic analysis. • Delete all unauthorised user accounts and credentials made by the attacker. • Close the firewall ports being exploited and segment the network. • Ensure core systems and configurations are free of compromise through checks.

Recovery	• Restore systems to normal operations through controlled phases. • Monitor privileged account activities with more security for an observation period. • Test and ensure full system functionality before returning fully to production. • Provide regular progress reports to leadership and stakeholders until the recovery is successful.
Lessons Learned	• Conduct a post-incident review to identify areas for improvement and response effectiveness. • Deliver a comprehensive report regarding the attack, mitigations used and recommendations for improvement. • Update the current security policies and privileged access management procedures. • Adjust staff training programs to highlight the importance of privileged account security.

Appendix E

CYBER SENTINEL INC. COMPLIANCE AND LEGAL OBLIGATIONS

This appendix outlines the key legal, regulatory, and compliance obligations that Cyber Sentinel Inc. must adhere to in the event of a cybersecurity incident. The following Australian laws and standards mandate incident preparation, breach response, and reporting duties.

Compliance and Legal Obligations

Privacy Act 1988 (Commonwealth Government of Australia)
The cornerstone of Australian privacy law, regulating the handling of personal information by government agencies and organizations with annual turnover above $3 million.

- **Reporting requirements** – Organizations must take reasonable steps to protect personal information and notify affected individuals and the OAIC if a breach is likely to cause serious harm.
- **Learn more** – https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act

Notifiable Data Breaches (NDB) Scheme
An amendment to the Privacy Act requiring mandatory breach notification when personal data is involved.

- **Reporting requirements** – Notify the Office of the Australian Information Commissioner (OAIC) and affected individuals within 30 days of becoming aware of an eligible breach.
- **Learn more** – https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme

Telecommunications (Interception and Access) Act 1979
Outlines obligations around accessing and protecting telecommunications content.

- **Reporting requirements** – Interception or unauthorised access to communications data may trigger mandatory reporting and coordination with the Australian Federal Police.
- **Learn more** – https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/telecommunications-interception-and-surveillance

Copyright Act 1968 (Commonwealth Government of Australia)
Applies to breaches involving unauthorized access, duplication, or distribution of proprietary content, including R&D and internal documents.

- **Reporting requirements** – Infringement or data theft may warrant legal action under intellectual property laws.
- **Learn more** – https://www.legislation.gov.au/C1968A00063/latest/text

Corporations Act 2001 (Commonwealth)
Governs financial reporting and operational risk management obligations for corporations in Australia.

- **Reporting requirements** – Directors must disclose material cyber risks or incidents that impact corporate performance or compliance.
- **Learn more** – https://www.legislation.gov.au/Series/C2004A00818

Work Health and Safety Act 2011 (Commonwealth Government of Australia**)**
Relevant to cases where cyber incidents may lead to workplace harm, e.g., psychosocial harm from data exposure.

- **Reporting requirements** – Organizations must assess and respond to any WHS-related risks caused by cyber breaches.
- **Learn more** – https://www.legislation.gov.au/Details/C2011A00137

Protective Security Policy Framework (PSPF) – Commonwealth Government of Australia
Provides guidance on physical, personnel, and information security for Australian government agencies and contractors.

- **Reporting requirements** – Serious or repeated failures to comply with protective measures should be reported to the Attorney-General's Department or other authorities.
- **Learn more** – https://www.protectivesecurity.gov.au

Essential Eight Maturity Model (Australian Cyber Security Centre)
Outlines strategies to mitigate cyber threats based on a risk-informed maturity model.

- **Reporting requirements** – Breaches may require ACSC coordination if critical infrastructure or high-value assets are involved.
- **Learn more** – https://www.cyber.gov.au

Industry-Specific Regulations

Cyber Sentinel Inc. complies with industry-specific regulations relevant to the sectors we serve. These regulations include mandatory requirements for incident response, breach notification, and data protection. For full legal context, refer to the Compliance and Legal Obligations section above.

PCI DSS (Payment Card Industry Data Security Standard)

Applies to entities handling credit card data, requiring incident response plans and immediate breach notifications.

- **Reporting requirements –** PCI DSS requires entities have an incident response plan and alert effected parties immediately. PCI DSS 3.2.1, released on May 2018, marks the latest version.
- You may want to set up an arrangement with an independent Payment Card Industry Forensic Investigator (PFI) to call if you need outside expertise.
- **Learn more –** https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf

NERC/CIP (Critical Infrastructure Protection)

Applies to cybersecurity in the bulk electric system, requiring reporting of security incidents affecting critical infrastructure.

- **Reporting requirements –** Reliability standards require the reporting of cyber security incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).
- **Learn more –** https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

SOX Sarbanes-Oxley (SOX)

Requires disclosure of cyber risks impacting financial reporting, relevant to publicly traded clients.

- **Reporting requirements –** Companies must disclose failure of security safeguards and security breaches to SOX auditors.
- **Learn more –** https://www.sarbanes-oxley-101.com/

Geographic Regulations

The core operations of Cyber Sentinel Inc. are based in Australia, where we comply with national privacy and cybersecurity laws as detailed in the Compliance and Legal Obligations section. For projects involving clients or data subjects in other regions, we acknowledge and consider applicable regulations such as:

EU General Data Protection Regulation (GDPR)

Any organization dealing with EU citizens' Personally Identifiable Information is obligated to meet standards for effective data protection, adequate security measures, and privacy by design to comply with EUGDPR.

- **Reporting requirements –** Under GDPR, breach notification is mandatory in all member states where a data breach is likely to result in a risk for the rights and freedoms of individuals. This must be done within 72 hours of first having become aware of the breach. Data processors are required to notify their customers, the controllers, without undue delay after first becoming aware of a data breach.
- **Learn more –** https://www.eugdpr.org/key-changes.html

UK Cyber Essential

Contractors in the UK that handle sensitive or personal information must receive Cyber Essentials Certification to demonstrate understanding and enforcement of privilege management.

- **Reporting requirements –** UK Cyber Essentials uses external auditors to confirm compliance with the security framework and award certificates.
- **Learn more –** https://www.cyberessentials.ncsc.gov.uk/

United Arab Emirates National Electronic Security Authority (NESA)

Requires government entities and businesses in critical sectors closely control and protect privileged accounts.

- **Reporting requirements –** NESA compliance involves a maturity-based self-assessment and allows for external auditing, testing and even intervention if activities pose a significant threat to national security.

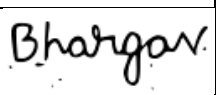
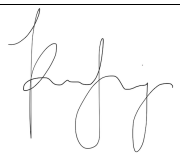
The geographic and industry-specific regulations outlined in this security maaster plan are adapted from Delinea's Cybersecurity Incident Response Plan Template (2025).

Appendix E

GROUP DECLARATION SHEET

Assignment Title:
Assignment 2 Security Master Plan

Group Name:
Cyber Sentinel Inc.

Member's Names	**Brief Description of Tasks** *(Details would be in the individual accounting spreadsheet)*	**Contribution to the total work**	**Date signed**	**Signature**
Damon Duffy 34144772	• Contributed across all report sections, particularly in risk identification, asset classification, and threat control practices • Primary focus on Section 3.0 (Understanding Information Security) and Section 5.0 (Risk Assessment) • Helped consolidate Appendices A–C, especially in mapping technical risks to infrastructure	33.3%	25/07/2025	
Bhargav Raj Dutta 34834517	• Participated in drafting, data validation, and ensuring consistency across sections • Key focus on Section 3.0 (Understanding Information Security) and Section 5.0 (Risk Assessment) • Collaborated on the Incident Response Plan (Appendix D) and helped review the technical and procedural risk sections across the report	33.3%	25/07/2025	
Klaryss Puno 35210149	• Involved in every stage of the report's development, from initial planning to final editing • Focused on Section 2.0 (Introduction) and Section 6.0 (Risk Management) • Led the document formatting, APA referencing, and final integration of Appendices F and the presentation slides	33.3%	25/07/2025	
Total percentage		100%		

All group members were actively involved in all areas of the Security Master Plan, including research, writing, risk analysis, table development, formatting, and cross-checking references. Each member contributed to every major section (1.0–6.0) and supported the preparation of Appendices (A–F). The team also jointly developed and reviewed the Incident Response Plan (Appendix D) and ensured that findings aligned with industry standards, and legal compliance requirements. In addition, all members also showed willingness to participate and prepare for the oral presentation of the security master plan.