APRIL 4, 2024

SECURITY MASTER PLAN

ZAINA SHAHID – 34669919

PETROCOMPASS TECHNOLOGIES

Table of Contents

EXECUTIVE SUMMARY

This document presents a comprehensive security master plan for PetroCompass Technologies to protect its critical assets and ensure business continuity in the oil and gas industry. It outlines a risk-based approach to identifying and mitigating potential threats across technical, physical, human resource, and policy/procedure domains. The plan emphasizes robust security management practices aligned with industry standards, including asset identification, risk management, threat detection, and incident response protocols. Key recommendations focus on implementing strong access controls, regular software/hardware updates, security awareness training, formal incident response planning, and continuous policy review. By proactively adopting this security plan, PetroCompass can enhance data security, minimize breach risks, prevent financial losses, and bolster its reputation for safeguarding valuable client information.

INTRODUCTION

PetroCompass Technologies is a medium industrial company that specializes in designing and selling tailored hardware and software for the oil and gas industry. The company is led by a CEO and a team of professionals who take control of critical operations for its consistent expansion and prosperity.

This document looks at managing information security, which is one of the main areas of operation for PetroCompass Technologies, by identifying possible risks to the company's assets and providing an overall risk assessment. It introduces a stepwise strategy for asset shield, which primarily comprises a risk assessment, assessment of factors such as impact likelihood, vulnerability likelihood, and cost-benefit analysis. The aim is to assist in the development of a BIA contingency plan for PetroCompass Technologies.

The report evaluates the various elements of potential risks, that is physical, technical, human resource, and policy and procedural, and proposes tactical actions to protect the assets of the agency. It defines and arranges assets that may be at risk by effective indictment and criteria weighting, considering possible effects on earnings, profits, and customer relations.

Mission:

PetroCompass Technologies is a company whose goal is to provide the industry with software and hardware solutions that are specifically designed for the needs of oil and gas. We are always in pursuit of the best quality products and services that help our clients to provide safe and efficient work environment for their employees. Simplicity and efficiency are the key points in our activities of seismic data analysis. We use advanced technologies to provide access to the information about the new sites where oil and gas could be extracted. Through relentless innovation and unwavering dedication, we aim to be the trusted partner in navigating the complexities of the energy sector, driving sustainable growth and success for our clients worldwide.

Vision:

Our goal is to exceed customer expectations by providing them with premium products and services, eventually becoming the leading supplier of seismic data processing and monitoring solutions to the oil and gas industry. Our main objective is to satisfy our customers which we achieve by developing user-friendly and efficient solutions to all our clients. Our goal is to be the industry leader in providing user-friendly software, making seismic processing easier but keeping our clients at the top of the competition in the fast-paced energy sector.

Team Structure and Responsibilities:

Zaina Shahid – CEO & Director Sales and Products

The CEO position in the organization of PetroCompass Technologies is held by the strategic management head, Zaina, who has the widest authority. It is her responsibility that all workers be involved equally in discussions and the team focus being on the ultimate goal. Acting as the final decision-maker in the event of disagreements, Zaina embodies organizational leadership, navigating conflicts, and safeguarding the company's reputation. Additionally, as the spokesperson for PetroCompass, Zaina represents the company's values and vision to external stakeholders.

The Director of Sales & Product, also held by Zaina, is responsible for driving the company's revenue growth and product innovation. Overseeing sales, marketing, and product development departments, Zaina provides strategic guidance and ensures alignment with the company's objectives. Directly managing key personnel such as the Software Manager, Data Processing Manager, and Support & Training Manager, Zaina plays a critical role in shaping the direction of PetroCompass's offerings.

Contact : ZAINASHAHID@PETROCOMPASS.AU.COM | +98 7635 6731 23

Ansh Babbar – CIO & Director Back Office

Ansh, in the role of Back Office Director, makes sure the administrative procedures that enable PetroCompass to work smoothly are in place. From providing leadership to HR, accounting, and finance to advising on the matters of these departments, Ansh makes sure that PetroCompass stays efficient and compliant. Ansh directly manages the finance manager, HR manager, and building and maintenance manager to ensure that these functions of PetroCompass run smoothly. Ansh also undertakes the role of the Chief Information Officer (CIO) who is in charge of the IT infrastructure of PetroCompass.Working closely with the CSO, Ansh is responsible for the IT security threats and the IT team's advice on all IT aspects, which helps in PetroCompass's technical advancement.

Contact : ANSHBABBAR@PETROCOMPASS.AU.COM | +98 9274 1245 90

Saahir Akbar – CSO & Legal Officer

Sahir, the head of security at PetroCompass, is accountable for guarding the entire company's security. Working in close collaboration with the CIO, Sahir deals with the security issues and is responsible for the company's safety in the physical and personal sense. Being the PetroCompass's advisor in general security issues, Sahir is the person who makes sure that the company will have a good name and reputation by helping maintain its integrity.

Sahir also serves as the Legal Officer, providing guidance on the legal and ethical implications of company decisions. Responsible for documenting meeting minute, Sahir ensures that PetroCompass operates within the bounds of the law and upholds its ethical obligations.

Contact : SAAHIRAKBAR@PETROCOMPASS.AU.COM | +98 6359 7363

RISK ANALYSIS

The process of locating and evaluating possible challenges that can have a negative impact on important business efforts or projects is known as risk analysis(Yasar & Rosencrance, 2023). This process is done to help organizations avoid or mitigate those risks. A business conducts risk analysis to gain a better understanding of potential outcomes, the financial consequences of those outcomes, and the actions that may be taken to reduce or eliminate such outcomes(Hayes, 2024).

In this section, the management team conducts a risk assessment for PetroCompass Technologies and presents a comprehensive risk analysis for each identified risk area. The risk analysis table concentrates on four primary domains: Technical, Human, Physical, and Processes and Procedures risks.These countermeasures are meticulously examined across various scenarios to ensure their effectiveness and reliability in addressing the respective risks. The team thoroughly evaluates each countermeasure to provide robust and dependable solutions to the potential risks faced by the organization.

1.1 TECHNICAL RISKS IDENTIFICATION & ANALYSIS:

Threat	Affect	Countermeasures
Unauthorized Access to Monitoring Software	Unauthorized access to SensorDrill and MeasureMe software could lead to problems . Tampering with monitoring software can disrupt drilling and pumping operations, causing delays and financial losses.	Determine the implementation of strong cybersecurity protocols, such as end-to-end encryption and safe login processes . Regularly update software and hardware components to patch vulnerabilities.
Unauthorized Use of Shake and Quake Software	Seismic data is processed and interpreted using this program. The software in question is extremely important to the business's procedures, so any problems with it or security breaches could have major consequences.	To fix any possible vulnerabilities, apply software updates and patches on a regular basis. Use strong encryption for all data transfers and keep an eye out for any strange activities.
Storage of the data along with data backup.	Physical damage or theft could potentially affect the data processor room's physical tapes as well as the methods and procedures utilized for data backup and storage. Additionally, there may be a chance of losing data if these	Make sure backups are consistently verified for successful restoration. Physical backup tapes should be kept safe and in an enclosed space to avoid harm. For further security, think about backups stored in the cloud

	backup procedures are unsuccessful for whatever reason.	or storage elsewhere. Make extra copies of your data backups on a regular basis .
Lack of automated OS Patching.	Considering that OS patching is off automatically. Systems may become exposed to safety hazards as a result, which these patches attempt to fix. These potential hazards could include malware infections with unprotected patches and system vulnerabilities that could result in data breaches.	Maintain compatibility with current systems while updating and patching operating systems and other software regularly. Inform staff members about standard practices for cybersecurity, like avoiding dubious websites and reporting any strange activity.
Inconsistent Operating System Versions	Varied operating system versions across client computers increase complexity and compatibility issues, potentially leading to security vulnerabilities and operational inefficiencies.	Migrate all client computers to a single version of Windows 10 Pro to ensure uniformity and compatibility.

1.2 PHYSICAL RISK IDENTIFICATION & ANALYSIS:

This section presents a strategic approach to managing physical risks within the organization. It addresses potential threats such as unauthorized access, theft, vandalism, natural disasters, and physical security breaches. The focus is on maintaining responsiveness, proactive planning, and regular reviews to ensure physical security measures remain effective against changing threat landscapes, alterations in the physical environment, and the shifting needs of business operations.

Threat	Affect	Countermeasures
Lack of Air Conditioning in Wiring Closets	There is no air conditioning in the wiring closets due to their size and location. The wiring closets contain router and switches, which tend to produce a lot of heat. The lack of air conditioning can increase the temperature of the room drastically, causing failure of equipment or an electrical fire.	Install air conditioning units in wiring closets. Use automatic thermostats to monitor and adjust temperature. Ensure adequate ventilation. Consider alternative cooling methods like liquid cooling.
Unlocked Server Rooms and Wiring Closets	The server room and wiring closet is left unlocked during the day to facilitate easy access for the IT staff. This can result in access by unauthorized personnel, who can gain control of the networking equipment and servers, which hold a lot of sensitive information. This data can easily be accessed, downloaded, and sold to our competitors for a monetary gain.	Keep server rooms and wiring closets always locked. Implement access control systems. Use CCTV cameras and data logging for monitoring. Require escorts or security personnel for access.
Lack of Security at the Cargo Lifts	Though there is a requirement to obtain contractor badges to access the cargo lifts, they are not escorted in or out meaning an outsider can easily enter the building premises if they take the cargo lift from the car park	Use access cards to control lift operation. Ensure access cards are issued against national identity card and monitored by security personnel. Implement CCTV surveillance.
Client Data is backed up on Physical Tapes	In the event of an uncontrolled fire, the tapes are very likely to be destroyed which can result in	Implement the 3-2-1 backup rule. (Vanover, 2024)

	major discrepancies to the day-to-day operations of the business.	Store data in multiple locations and media types. Keep one copy off-site in a secure location. Regularly test backup and recovery procedures.
General Security Concerns Around Visitors	Visitors are escorted into the company premises by the employee they are meeting, but once the meeting ends, the employee is not required to escort them out. This poses a significant security risk as visitors could potentially gain access to sensitive areas or attempt to steal equipment. There is also the risk of competitors disguising themselves as clients to gain access to confidential information, leading to potential setbacks and losses.	Escort visitors to sensitive areas. Implement access control for visitor entry and exit. Use CCTV cameras for monitoring. Ensure employees are trained on security protocols and visitor management.

1.3 HUMAN RISK IDENTIFICATION & ANALYSIS:

This section introduces a strategic methodology for mitigating human risks throughout the organization. It encompasses risks associated with human factors such as insider threats, social engineering, human errors, and workforce negligence.

Threat	Affects and Analysis	Prevention / Countermeasures
Employees and Contractors with Access to Sensitive Data and Systems	Company reputation to stakeholders and public eye may be affected if data is breached and leaked. Employees can potentially misuse their access privileges to confidential information or systems, with either malicious intent or without.	Implement card access control for entry restricted to IT staff only - Educate staff on proper access control procedures PoLP (principle of least privilege) should be put in action Users should only be granted the level of access needed to complete their assigned tasks.
Unsecured Physical Access Points	The cargo lift may be used after working hours with the permission of the security office and the doors from the lift lobby to the office area are locked by the last person who leaves at the end of the busy working day. Such practices could provide keys to unauthorized persons to enter the restricted areas of the building.	Upgrade security measures to secure all physical access points - Implement badge scanning system for real-time monitoring of entries and exits.
Lack of Password Security Measures	There is no mandatory controls (enforced periodic password changes for every employee) Increased risk of unauthorized access and data breaches	Enforce mandatory password changes, minimum complexity requirements, and multi-factor authentication Provide regular training on password security

Inadequate Visitor Control	Visitors are accompanied upon entry but lack escort upon exiting, similarly, vendors and contractors are required to acquire a badge yet are not accompanied upon entry or exit. Increased risk of unauthorized access to sensitive areas or information	Escort all visitors and ensure sign-out procedures are followed Accompany contractors and vendors, minimizing access to sensitive areas
Use of Short-term Contract Staff	Extensive reliance on contract staff to fulfill temporary staffing needs may lead to individuals with limited loyalty or familiarity with the company's procedures gaining access to sensitive data or systems. Increased risk of intellectual property theft and data breaches	Provide security training to contract staff, terminate access rights promptly upon contract completion Organizations should conduct background checks on the employment agency, assessing their reputation, reliability, and credibility. Additionally, organizations should conduct background checks and individual interviews on candidates recommended by the employment agency to ensure they meet the organization's requirements.
Unguarded Server Rooms	Company perception to stakeholders and public eye may be affected if data is breached and leaked	Install card access control restricted to IT staff only - Educate staff on access control procedures
Cleaners Left Unlocked Server Room	Potential unauthorized access leading to data tampering or theft	Implement biometric access controls and CCTV surveillance Enforce multi-factor authentication for accessing sensitive systems

Lack of Security Awareness among Employees	Increased risk of phishing attacks and data breaches	Provide regular training on identifying phishing attempts and secure data handling practices
Tampering with Delivered Goods	Increased risk of data breaches and physical security breaches	Conduct thorough background checks on suppliers and maintain chain of custody for delivered goods Implement physical security measures and surveillance
Vendor Management	Increased risk of third-party breaches and compliance violations	Regularly assess and monitor subcontractors for compliance and security standards Implement contractual obligations and enforce security protocols
Contracted and temporary staff have same access as permanent staff.	Increased risk of data breaches and loss of confidential information once they leave.	Restrict access to information for temporary staff, limit privileges to necessary duties. Implement encryption or Privileged Access Management (PAM) for added data protection.
Upper management offices vulnerable to breaches by cleaners after hours due to open-plan layout and lack of office locking policy.	Risk of unauthorized access to sensitive information and potential data breaches.	Enforce office locking policy for all employees before leaving work. Employ security officers for regular patrols to ensure compliance and enhance physical security measures.

1.4 POLICIES/PROCEDURES AT RISK:

The agenda presents a strategic methodology for developing and implementing a comprehensive security framework within the organization. This framework will consist of security policies and procedures carefully crafted to align with the specific requirements of the organization.

POLICY / PROCEDURE	THREAT	COUNTERMEASURE
Password Management Policy	Password policies are only updated following security incidents, potentially leading to outdated policies during periods without incidents.	Regular intervals for policy reviews safeguard against outdated security measures and enhance operational performance.
Standardized Operating System	Managers can choose between any Windows OS version for laptops, causing software management complexity and compatibility issues.	Maintain a single standardized OS within the office network to streamline software management. Any non-standard OS should operate on a separate network for simplified software updates.
Information Security Policy Plan	Lack of an information security policy plan results in unclear guidelines for staff actions in various situations.	Maintain a consistently updated information security policy filled with incident reports to guide staff actions.
Access Control for Car Park Entry	Lack of access control for car park entry allows unauthorized individuals to enter the building.	Implement access control measures for car park entry to prevent unauthorized access.
Incident Response Policy	Lack of a straightforward incident response plan can result in slow or ineffective responses to cybersecurity incidents, leading to much larger and irreversible damage.	Establish a detailed incident response policy outlining immediate actions, communications, and post-incident reviews. Distribute the roles and responsibilities to ensure swift and effective responses.
Remote Work Policy	Lack of a remote working policy that includes the security measures that must be followed	Establish a remote work policy with requirements for secure home networks, VPN usage for

	for off-site work can result in a higher frequency of security breaches.	accessing company networks, and guidelines for securing remote work devices.

SECURITY MANAGEMENT PRACTICES:

The primary objective of PetroCompass Technologies' security management practices is to establish a robust foundation for the company's comprehensive cybersecurity strategy. The information and processes developed through these procedures will serve as the backbone for asset identification, risk management, and threat detection and response mechanisms within the organization(Habte, 2022).

PetroCompass Technologies' information security management approach encompasses the implementation of industry best practices and adherence to recognized standards outlined by NIST (National Institute of Standards and Technology). These measures are specifically designed to mitigate threats to the organization's data and ensure the maintenance of data confidentiality, integrity, and availability.

NIST, under the U.S. Department of Commerce, provides guidance through its Cybersecurity Framework, which assists businesses of all sizes in better understanding, managing, and reducing their cybersecurity risks, ultimately protecting their networks and data from potential threats(*Understanding the NIST Cybersecurity Framework*, 2022).

This table presents a comprehensive risk analysis framework tailored specifically for PetroCompass Technologies. It serves as a structured approach to identifying, assessing, and mitigating potential risks across various domains, including technical, physical, human, and policy/procedure-related risks.

Risk Identification: The table identifies specific risks that PetroCompass Technologies may face within each risk domain. These risks range from unauthorized access to monitoring software and inconsistent operating system versions in the technical realm, to lack of air conditioning in wiring closets and unlocked server rooms in the physical domain, to employees and contractors with access to sensitive data and systems, and lack of password security measures in the human risk domain.

Best Practices: For each identified risk, the table outlines industry-standard best practices that PetroCompass Technologies should consider implementing. These best practices are derived from established guidelines, frameworks, and expert recommendations, ensuring that the organization aligns its risk mitigation efforts with proven methodologies.

Due Diligence: This section highlights the necessary due diligence measures that PetroCompass Technologies should undertake to effectively address the identified risks. These measures may include conducting security audits, implementing data backup procedures, assessing compatibility issues, or conducting background checks on personnel.

Considerations: The table also presents relevant considerations for PetroCompass Technologies to take into account when implementing risk mitigation strategies. These considerations may involve factors such as maintaining strict access controls, ensuring user training and support, implementing disaster recovery plans, or addressing company reputation and data breach risks.

Metrics/Measurements: To effectively monitor and evaluate the success of risk mitigation efforts, the table provides suggested metrics and measurements for each risk area. These metrics may include frequency of software updates, successful login attempts, encryption strength, temperature monitoring, access logs, security incident reports, password strength scores, and compliance audit results.

2.1 TECHNICAL RISKS:

Technical Risk	Best Practices	Due Diligence	Considerations	Metrics/ Measurements
Unauthorized Access to Monitoring Software	Implement strong cybersecurity protocols (e.g., encryption, secure login processes), regularly update software and hardware components for patching vulnerabilities	Ensure end-to-end encryption for data transfers, verify the integrity of software updates and patches	Maintain strict access controls, conduct regular security audits	Frequency of software updates, successful login attempts, encryption strength
Unauthorized Use of Shake and Quake Software	Apply software updates and patches regularly, use strong encryption for data transfers	Implement data backup and storage procedures, monitor for unusual activities	Regularly verify data backups for successful restoration, ensure physical security of backup tapes	Frequency of software updates, frequency of backup verification, incidence of unusual activities
Lack of Automated OS Patching	Maintain compatibility with current systems, regularly update and patch operating systems	Educate staff on cybersecurity best practices, report any suspicious activity	Conduct regular cybersecurity training for staff members, monitor patching process automation for effectiveness	Frequency of OS updates, staff training completion rates, incidents of suspicious activity
Inconsistent Operating System Versions	Migrate all client computers to a single version of Windows 10 Pro	Assess compatibility issues and plan migration accordingly, consider user impact	Ensure user training and support during migration process, assess potential impact	Percentage of client computers migrated, user feedback on migration process, operational impact

			on existing operations	

2.2 PHYSICAL RISKS:

Physical Risk	Best Practices	Due Diligence	Considerations	Metrics/Measurements
Lack of Air Conditioning in Wiring Closets	Install air conditioning units in wiring closets. Use automatic thermostats to monitor and adjust temperature	Ensure adequate ventilation. Consider alternative cooling methods like liquid cooling	Proper sizing and placement of AC units. Redundancy and backup cooling systems.	Temperature monitoring. Equipment failure rates. Energy consumption.
Unlocked Server Rooms and Wiring Closets	Keep server rooms and wiring closets always locked. Implement access control systems.	Use CCTV cameras and data logging for monitoring. Require escorts or security personnel for access.	Physical security barriers and alarms. Background checks for personnel access. Incident response plan	Access logs Security breach incidents.
Lack of Security at the Cargo Lifts	Use access cards to control lift operation. Ensure access cards are issued against national identity card.	Implement CCTV surveillance. Monitor access by security personnel.	Visitor management protocols. Secure storage of access cards. Tracking of access card usage	Unauthorized access incidents. CCTV footage review.
Client Data is backed up on Physical Tapes	Implement the 3-2-1 backup rule. Store data in multiple locations and media types	Keep one copy off-site in a secure location. Regularly test backup and recovery procedures	Encryption and access controls for backups. Disaster recovery plan	Backup success rates Recovery time and data integrity
General Security Concerns Around Visitors	Escort visitors to sensitive areas. Implement access control for visitor entry and exit	Use CCTV cameras for monitoring.	Visitor identification and vetting process.	Visitor access incidents.

		Ensure employees are trained on security protocols.	Restricted areas and need-to-know basis. Secure storage of visitor logs.	

2.3 HUMAN RISKS:

Human Risk	Best Practices	Due Diligence	Considerations	Metrics/Measurements
Employees and Contractors with Access to Sensitive Data and Systems	Implement principle of least privilege (PoLP), provide access control training, implement card access control for restricted areas	Conduct background checks on employees and contractors	Company reputation, data breach risk	Access audit logs, number of incidents related to unauthorized access
Unsecured Physical Access Points	Upgrade security measures, implement badge scanning system for monitoring entries/exits	Conduct physical security audits	Monitoring and controlling physical access	Number of unauthorized entries, security incident reports
Lack of Password Security Measures	Enforce password complexity, multi-factor authentication, provide password security training	Assess current password policies and practices	Data breach risk, unauthorized access	Password strength scores, number of failed login attempts
Inadequate Visitor Control	Escort visitors, contractors, and vendors, minimize access to sensitive areas	Review visitor management procedures	Unauthorized access risk	Number of unescorted visitors, areas accessed by visitors
Use of Short-term Contract Staff	Conduct background checks, provide security training, terminate access	Assess employment agency credibility, interview candidates	Intellectual property theft, data breach risk	Contract staff security incidents, contract staff turnover rate

	promptly after contract			
Unguarded Server Rooms	Implement card access control, provide access control training	Assess server room physical security	Data breach risk, company reputation	Number of unauthorized entries, security incident reports
Cleaners Left Unlocked Server Room	Implement biometric access controls, CCTV surveillance, multi-factor authentication	Assess cleaning staff security procedures	Unauthorized access, data tampering risk	Number of unauthorized entries, security incident reports
Lack of Security Awareness among Employees	Provide regular security awareness training	Assess current security awareness levels	Phishing attack risk, data breach risk	Number of successful phishing simulations, security incidents
Tampering with Delivered Goods	Conduct supplier background checks, implement physical security measures	Assess supply chain security procedures	Data breach risk, physical security risk	Number of security incidents related to delivered goods
Vendor Management	Regularly assess and monitor subcontractors, implement security contracts	Conduct due diligence on subcontractors	Third-party breach risk, compliance violations	Number of third-party security incidents, compliance audit results
Contracted and Temporary Staff Access	Restrict access privileges, implement encryption or Privileged Access Management (PAM)	Assess temporary staff access procedures	Data breach risk, loss of confidential information	Access audit logs, number of security incidents related to temporary staff
Upper Management Office Security	Enforce office locking policy, employ security patrols, enhance physical security measures	Assess upper management office security procedures	Unauthorized access risk, data breach risk	Number of unauthorized entries, security incident reports

2.4 POLICY/PROCEDURES RISKS:

Policy/Procedure Risk	Best Practices	Due Diligence	Considerations	Metrics/Measurements
Password Management Policy	Regularly review and update password policies, implement password strength requirements	Assess current password practices and incident history	Data breach risk, compliance	Password strength scores, number of failed login attempts
Standardized Operating System	Implement a single, standardized OS across the network, separate non-standard OS systems	Assess software management challenges and compatibility issues	Software management complexity, compatibility risks	Number of software issues, compatibility incidents
Information Security Policy Plan	Regularly update the policy with incident reports, provide training and guidance	Assess current security practices and incident response effectiveness	Clear staff guidelines, security incident mitigation	Number of security incidents, staff awareness levels
Access Control for Car Park Entry	Implement access control measures (e.g., badges, biometrics)	Assess current physical access vulnerabilities	Unauthorized access risk, building security	Number of unauthorized entries, security incident reports
Incident Response Policy	Establish a detailed incident response plan, assign roles and responsibilities	Assess current incident response capabilities and effectiveness	Swift and effective incident response, damage mitigation	Response times, incident resolution rates, post-incident reviews
Remote Work Policy	Implement secure network, VPN, and device requirements for remote work	Assess current remote work security practices and risks	Data breach risk, unauthorized access	Number of remote work-related incidents, compliance audits

Our organization uses benchmarking to ensure that high standards of due care and diligence are met. By using benchmarking, one can make sure that the previously mentioned areas of concern are protected from outside threats and that the right actions are taken in the event of a crisis.

RISK ASSESSMENT:

The practice of identifying possible risks and predicting on the outcomes of a disaster or hazard is known as risk assessment. There are various risks to take into account, and each risk may have a variety of potential outcomes either within or as a result of it(*Risk Assessment | Ready.gov*, n.d.).

3.1 ASSET LIST:

To facilitate a structured risk analysis and assessment approach, PetroCompass Technologies has identified and categorized its information assets into distinct categories. These categories enable the organization to account for varying levels of data sensitivity associated with different types of assets.

Our assets include both tangible elements like hardware and physical infrastructure, as well as intangible assets such as software, data repositories, and human resources. Identifying these assets helps us understand what critical components need protection and where we should prioritize our security efforts.

Asset List	
IBM Blade Center	Networking
Cisco 3750E	Networking
Cisco 3845 ISR	Networking
Cisco 2960 Access Switch	Networking
Konica Minolta C350 MFC	Hardware
Cisco 7941G IP Phone	Hardware
Cisco 1242AG	Networking
Big Lake ISP	Networking
SensorDrill	Software
MeasureMe	Software
Shake and Quake	Software
Project 2 (In Research and Development)	Software
Dell Optiplex 360	Hardware
Windows 10 Pro	Software
Windows 8.1	Software
Windows Server 2016	Software
Ubuntu 16.04	Software
Red Hat Enterprises	Software
Virtual Machines	Software
Microsoft Outlook 2016	Software
Microsoft Office 2016	Software
Dell Inspiron 15 Laptop	Hardware

Dell Precision 3590 Workstation	Hardware
HP Proliant Gen9 Servers	Hardware
Symantec Backup Executive	Software
HP 1/8 G2 Tape Autoloader	Hardware
McAfee Antivirus	Software
Domain Controller Server	Hardware
Printer Server	Hardware
File Server	Hardware
Web Server	Hardware
Data Backup Tapes	Hardware
Seismic Data Processing Servers	Data
Customer Data	Data
Employee Data	Data
Financial Data	Data
R&D Data	Data
Vendor Data	Data
Contractor Data	Data
Access Control Procedures	Procedure
Disaster Recovery Plan	Procedure
Contractor Onboarding Procedure	Procedure
Client Onboarding Procedure	Procedure
Vendor Onboarding Procedure	Procedure
Contractor Offboarding Procedure	Procedure
Client Offboarding Procedure	Procedure
Vendor Offboarding Procedure	Procedure
Clean and Mean Pty Ltd.	People
Computex Pty Ltd.	People
Printmaster Pty Ltd.	People
PeopleRus Human Resource Pty Ltd.	People
Hungerbuster Pty Ltd.	People
Chief Security Officer	People
Chief Information Technology Officer	People
Director Sales & Product	People
Division Head - Research and Development	People
Division Head - Software	People
Division Head - Data Processing	People
Division Head - Service and Technical Support	People
Director - Back Office	People
Manager Building and Maintenance	People
Manager Officer Administration	People
Manager Finance	People
Manager Human Resource	People
Manager Legal Department	People
Legal Officer	People
Staff	People

Xero	Software

3.2 INFORMATION WEIGHTED SCORE :

Conducting a Weight Criteria Analysis (WCA) was the next step. Three criteria will be used to evaluate the assets' impact on revenue, profitability, and public image. By adding the three scores, we can determine the asset's weighted score based on these three characteristics. Weighted scoring is a technique for setting project priorities that involves valuing each work numerically based on an effort-to-value ratio(*What Is Weighted Scoring? | craft.io*, 2023).

Formula for weighted score: Weighted Score = (Impact on Revenue * 30) + (Impact on Profitability * 40) + (Impact on Public Image * 30)

3.2.1 PEOPLE WCA:

People - Asset	Impact on Revenue (0-1)	Impact on profitability (0-1)	Impact on Public Image (0-1)	Weighted Score (0-1)
Clean and Mean Pty Ltd.	0.4	0.2	0.6	38
Computex Pty Ltd.	0.7	0.6	0.5	60
Printmaster Pty Ltd.	0.5	0.4	0.2	37
PeopleRus Human Resource Pty Ltd.	0.8	0.6	0.7	70
Hungerbuster Pty Ltd.	0.1	0.1	0.1	10
Chief Security Officer	0.9	0.8	0.8	83
CEO	1	0.9	1	96

Chief Information Technology Officer	0.9	0.8	0.8	83
Director Sales & Product	0.7	0.8	0.9	80
Division Head - Research and Development	0.8	0.8	0.5	71
Division Head - Software	0.7	0.8	0.4	65
Division Head - Data Processing	0.7	0.7	0.4	61
Division Head - Service and Technical Support	0.6	0.7	0.7	67
Middle Management	0.7	0.7	0.5	64
Legal Officer	0.8	0.5	0.7	65
Lower Staff	0.6	0.7	0.3	55

3.2.2 NETWORKING WCA:

Networking - Asset	Impact on Revenue	Impact on Profitability	Impact on Public Image	Weighted Score
Cisco 3750E	0.7	0.8	0.1	56
Cisco 3845 ISR	0.3	0.2	0.2	23
Cisco 2960 Access Switch	0.4	0.6	0.1	39
Cisco 1242AG	0.3	0.6	0.1	36
Big Lake ISP	0.4	0.6	0.3	45

3.2.3 HARDWARE WCA:

Hardware - Asset	Impact on Revenue	Impact on Profitability	Impact on Public Image	Weighted Score
Konica Minolta C350 MFC	0.2	0.3	0.2	24
Cisco 7941G IP Phone	0.3	0.2	0.4	29
Dell Inspiron 15 Laptop	0.7	0.7	0.3	58
Dell Precision 3590 Workstation	0.8	0.6	0.3	57
HP Proliant Gen9 Servers	0.6	0.7	0.1	49
HP 1/8 G2 Tape Autoloader	0.6	0.6	0.1	40
Domain Controller Server	0.6	0.7	0.2	52
File and Print Server	0.4	0.6	0.1	39
Web Server	0.7	0.5	0.3	50
Data Backup Tapes	0.6	0.5	0.3	47
Seismic Data Processing Servers	1	1	0.7	91
IBM Blade Center	1	1	0.8	94
VOIP Servers	0.6	0.6	0.5	62
Tape Array	0.7	0.6	0.6	63

3.2.4 SOFTWARE WCA:

Software - Asset	Impact on Revenue	Impact on profitability	Impact on Public Image	Weighted Score
SensorDrill	1	1	1	100
MeasureMe	1	1	1	100

Shake and Quake	1	1	0.5	85
Project 2 (In Research and Development)	1	1	0.9	97
Windows 10 Pro	0.7	0.6	0.2	51
Windows 8.1	0.7	0.6	0.2	51
Windows Server 2016	0.8	0.7	0.3	61
Ubuntu 16.04	0.1	0.1	0.1	10
Red Hat Enterprises	0.1	0.2	0.1	14
Virtual Machines	0.2	0.1	0.1	13
Microsoft Outlook 2016	0.2	0.4	0.5	37
Microsoft Office 2016	0.2	0.1	0.3	19
Symantec Backup Executive	0.2	0.1	0.1	13
McAfee Antivirus	0.4	0.2	0.5	35
Xero (Accounting Software)	0.7	0.6	0.3	54

3.2.5 DATA WCA:

Data - Asset	Impact on Revenue	Impact on profitability	Impact on Public Image	Weighted Score
Customer Data	1	1	1	100
Employee Data	1	1	1	100
Financial Data	0.8	0.8	1	86
R&D Data	0.9	0.9	0.8	87
Vendor Data	0.6	0.6	0.5	57
Contractor Data	0.7	0.8	0.7	74

3.2.6 PROCEDURE WCA:

Procedure - Asset	Impact on Revenue	Impact on profitability	Impact on Public Image	Weighted Score
Access Control Procedures	0.7	0.6	0.7	66
Disaster Recovery Plan	0.8	0.9	0.3	69
Contractor Onboarding Procedure	0.6	0.4	0.2	40
Client Onboarding Procedure	0.6	0.5	0.6	56
Vendor Onboarding Procedure	0.3	0.4	0.2	31
Contractor Offboarding Procedure	0.5	0.3	0.2	33
Client Offboarding Procedure	0.5	0.2	0.1	26
Vendor Offboarding Procedure	0.2	0.3	0.1	21

3.3 VULNERABILITY RISK ASSESSMENT:

To generate a risk rating, the next step is to perform a Vulnerability Risk Assessment (VRA). The vulnerability likelihood and asset impact value (weighted score) are used to compute the rating.
The process of locating, measuring, and ranking the flaws in an IT organization is known as vulnerability assessment. An assessment's objective is to identify vulnerabilities that could be used to breach organization(Dynatrace, 2024

Formula for VRA: Risk Rating Factor = Asset impact value * Likelihood

The table below shows our vulnerability assessment, where we identify potential threats, assess their likelihood and potential impacts, and calculate likelihood scores by multiplying likelihood and impact. This score helps us understand the severity of risks for each vulnerability.

3.3.1 PEOPLE VRA:

Asset	Asset Impact	Vulnerability	Likelihood	Risk Rating Factor
Clean and Mean Pty Ltd.	38	Insider threats, unauthorized access	0.6	22.8
		Network Attacks	0.1	3.8
		Identity Theft	0.6	22.8
		Human Errors	0.5	19
		Social Engineering	0.5	19
		Intellectual Property Theft	0.6	22.8
		Data Breaches	0.2	7.6
Computex Pty Ltd.	60	Insider threats, unauthorized access	0.8	48
		Network Attacks	0.3	18
		Identity Theft	0.7	42
		Human Errors	0.7	42
		Social Engineering	0.4	24
		Intellectual Property Theft	0.9	54
		Data Breaches	0.8	48
Printmaster Pty Ltd.	37	Insider threats, unauthorized access	0.5	18.5
		Network Attacks	0.2	7.4
		Identity Theft	0.5	18.5
		Human Errors	0.4	14.8
		Social Engineering	0.4	14.8
		Intellectual Property Theft	0.5	18.5
		Data Breaches	0.3	11.1

PeopleRus Human Resource Pty Ltd.	70	Insider threats, unauthorized access	0.9	63
		Network Attacks	0.4	28
		Identity Theft	0.8	56
		Human Errors	0.7	49
		Social Engineering	0.7	49
		Intellectual Property Theft	0.8	56
		Data Breaches	0.6	6
Hungerbuster Pty Ltd.	10	Insider threats, unauthorized access	0.2	2
		Network Attacks	0.1	1
		Identity Theft	0.2	2
		Human Errors	0.1	1
		Social Engineering	0.1	1
		Intellectual Property Theft	0.2	2
		Data Breaches	0	0
Chief Security Officer	83	Insider threats, unauthorized access	0.9	74.7
		Network Attacks	0.8	66.4
		Identity Theft	0.9	74.7
		Human Errors	0.8	66.4
		Social Engineering	0.8	66.4
		Intellectual Property Theft	0.9	74.7
		Data Breaches	0.7	58.1
CEO	96	Insider threats, unauthorized access	0.9	86.4
		Network Attacks	0.9	86.4
		Identity Theft	0.9	86.4
		Human Errors	0.9	86.4
		Social Engineering	0.9	86.4
		Intellectual Property Theft	0.9	86.4
		Data Breaches	0.8	76.8
Chief Information Technology Officer	83	Insider threats, unauthorized access	0.9	74.7
		Network Attacks	0.8	66.4
		Identity Theft	0.9	74.7
		Human Errors	0.8	66.4
		Social Engineering	0.8	66.4
		Intellectual Property Theft	0.9	74.7
		Data Breaches	0.7	58.1
Director Sales & Product	80	Insider threats, unauthorized access	0.8	64

		Network Attacks	0.6	48
		Identity Theft	0.7	56
		Human Errors	0.5	40
		Social Engineering	0.6	48
		Intellectual Property Theft	0.7	56
		Data Breaches	0.4	32
Division Head - Research and Development	71	Insider threats, unauthorized access	0.7	49.7
		Network Attacks	0.5	35.5
		Identity Theft	0.6	42.6
		Human Errors	0.5	35.5
		Social Engineering	0.5	35.5
		Intellectual Property Theft	0.6	42.6
		Data Breaches	0.3	21.3
Division Head - Software	65	Insider threats, unauthorized access	0.7	45.5
		Network Attacks	0.5	32.5
		Identity Theft	0.6	39
		Human Errors	0.5	32.5
		Social Engineering	0.5	32.5
		Intellectual Property Theft	0.6	39
		Data Breaches	0.3	19.5
Division Head - Data Processing	61	Insider threats, unauthorized access	0.6	36.6
		Network Attacks	0.4	24.4
		Identity Theft	0.5	30.5
		Human Errors	0.4	24.4
		Social Engineering	0.4	24.4
		Intellectual Property Theft	0.5	30.5
		Data Breaches	0.2	12.2
Division Head - Service and Technical Support	67	Insider threats, unauthorized access	0.7	46.9
		Network Attacks	0.5	33.5
		Identity Theft	0.6	40.2
		Human Errors	0.5	33.5
		Social Engineering	0.5	33.5
		Intellectual Property Theft	0.6	40.2
		Data Breaches	0.3	20.1
Middle Management	64	Insider threats, unauthorized access	0.7	44.8
		Network Attacks	0.5	32
		Identity Theft	0.6	38.4

		Human Errors	0.5	32
		Social Engineering	0.5	32
		Intellectual Property Theft	0.6	38.4
		Data Breaches	0.3	19.2
Legal Officer	65	Insider threats, unauthorized access	0.7	45.5
		Network Attacks	0.5	32.5
		Identity Theft	0.6	39
		Human Errors	0.5	32.5
		Social Engineering	0.5	32.5
		Intellectual Property Theft	0.6	39
		Data Breaches	0.3	19.5
Lower Staff	55	Insider threats, unauthorized access	0.6	33
		Network Attacks	0.4	22
		Identity Theft	0.5	27.5
		Human Errors	0.4	22
		Social Engineering	0.4	22
		Intellectual Property Theft	0.5	27.5
		Data Breaches	0.2	11

3.3.2 NETWORKING VRA:

Asset	Asset Impact	Vulnerability	Likelihood	Risk Rating Factor
Cisco 3750E	56	Outdated Firmware	0.5	28
		Default Credentials	0.6	33.6
		Unauthorized Access	0.9	50.4
		Network Attacks	0.7	39.2
		Data Exfiltration	0.8	44.8
		Distributed Denial of Service Attacks	0.9	50.4
Cisco 3845 ISR	23	Outdated Firmware	0.4	9.2
		Default Credentials	0.6	13.8
		Unauthorized Access	0.8	18.4
		Network Attacks	0.8	18.4
		Data Exfiltration	0.7	16.1
		Distributed Denial of Service Attacks	0.8	18.4
Cisco 2960 Access Switch	39	Outdated Firmware	0.4	15.6
		Default Credentials	0.6	23.4
		Unauthorized Access	0.8	31.2
		Network Attacks	0.9	35.1
		Data Exfiltration	0.7	27.3
		Distributed Denial of Service Attacks	0.8	31.2
Cisco 1242AG	36	Outdated Firmware	0.5	18
		Default Credentials	0.5	18
		Unauthorized Access	0.8	28.8
		Network Attacks	0.8	28.8
		Data Exfiltration	0.7	25.2
		Distributed Denial of Service Attacks	0.8	28.8
Big Lake ISP	45	Outdated Firmware	0.4	18
		Default Credentials	0.5	22.5
		Unauthorized Access	0.7	31.5
		Network Attacks	0.9	40.5
		Data Exfiltration	0.7	31.5
		Distributed Denial of Service Attacks	0.8	36

3.3.3 HARDWARE VRA:

Asset	Asset Impact	Vulnerability	Likelihood	Risk Rating Factor
Konica Minolta C350 MFC	24	Firmware Vulnerabilities	0.8	19.2
		Unpactched OS Software	0.7	16.8
		Unauthorized Access	0.7	16.8
		Data Breaches	0.9	21.6
		Malware Infection	0.8	19.2
		Outdated Firmware	0.6	14.4
Cisco 7941G IP Phone	29	Firmware Vulnerabilities	0.7	20.3
		Unpactched OS Software	0.6	17.4
		Unauthorized Access	0.7	20.3
		Data Breaches	0.8	23.2
		Malware Infection	0.9	26.1
		Outdated Firmware	0.6	17.4
Dell Inspiron 15 Laptop	58	Firmware Vulnerabilities	0.7	40.6
		Unpactched OS Software	0.9	52.2
		Unauthorized Access	0.9	52.2
		Data Breaches	0.8	46.4
		Malware Infection	0.9	52.2
		Outdated Firmware	0.7	40.6
Dell Precision 3590 Workstation	57	Firmware Vulnerabilities	0.8	45.6
		Unpactched OS Software	0.7	39.9
		Unauthorized Access	0.8	45.6
		Data Breaches	0.9	51.3
		Malware Infection	0.9	51.3
		Outdated Firmware	0.7	39.9
HP Proliant Gen9 Servers	49	Firmware Vulnerabilities	0.8	39.2
		Unpactched OS Software	0.7	34.3
		Unauthorized Access	0.8	39.2
		Data Breaches	0.8	39.2
		Malware Infection	0.9	44.1

		Outdated Firmware	0.7	34.3
HP 1/8 G2 Tape Autoloader	40	Firmware Vulnerabilities	0.8	32
		Unpactched OS Software	0.5	20
		Unauthorized Access	0.7	28
		Data Breaches	0.8	32
		Malware Infection	0.8	32
		Outdated Firmware	0.7	28
Domain Controller Server	52	Firmware Vulnerabilities	0.8	41.6
		Unpactched OS Software	0.7	36.4
		Unauthorized Access	0.9	46.8
		Data Breaches	0.9	46.8
		Malware Infection	0.8	41.6
		Outdated Firmware	0.7	36.4
File and Print Server	39	Firmware Vulnerabilities	0.8	31.2
		Unpactched OS Software	0.6	23.4
		Unauthorized Access	0.9	35.1
		Data Breaches	0.9	35.1
		Malware Infection	0.8	31.2
		Outdated Firmware	0.6	23.4
Web Server	50	Firmware Vulnerabilities	0.9	45
		Unpactched OS Software	0.8	40
		Unauthorized Access	0.9	45
		Data Breaches	0.9	45
		Malware Infection	0.9	45
		Outdated Firmware	0.7	35
Data Backup Tapes	47	Firmware Vulnerabilities	0.9	42.3
		Unpactched OS Software	0.7	32.9
		Unauthorized Access	0.9	42.3
		Data Breaches	0.9	42.3
		Malware Infection	0.8	37.6
		Outdated Firmware	0.7	32.9
Seismic Data Processing Servers	91	Firmware Vulnerabilities	0.8	72.8

		Unpactched OS Software	0.6	54.6
		Unauthorized Access	0.8	72.8
		Data Breaches	0.9	81.9
		Malware Infection	0.8	72.8
		Outdated Firmware	0.6	54.6
IBM Blade Center	94	Firmware Vulnerabilities	0.7	65.8
		Unpactched OS Software	0.7	65.8
		Unauthorized Access	0.8	75.2
		Data Breaches	0.9	84.6
		Malware Infection	0.7	65.8
		Outdated Firmware	0.6	56.4
VOIP Servers	62	Firmware Vulnerabilities	0.8	49.6
		Unpactched OS Software	0.8	49.6
		Unauthorized Access	0.9	55.8
		Data Breaches	0.8	49.6
		Malware Infection	0.9	55.8
		Outdated Firmware	0.6	37.2
Tape Array	63	Firmware Vulnerabilities	0.6	37.8
		Unpactched OS Software	0.5	31.5
		Unauthorized Access	0.7	44.1
		Data Breaches	0.8	50.4
		Malware Infection	0.4	25.2
		Outdated Firmware	0.5	31.5

3.3.4 DATA VRA:

Asset	Asset Impact	Vulnerability	Likelihood	Risk Rating Factor
Customer Data	100	Data Breaches	0.9	90
		Unauthorized Access	0.7	70
		Financial Fraud	0.8	80
		Intellectual Property Theft	0.7	70
Employee Data	100	Data Breaches	0.8	80
		Unauthorized Access	0.7	70
		Financial Fraud	0.6	60
		Intellectual Property Theft	0.8	80
Financial Data	86	Data Breaches	0.9	77.4
		Unauthorized Access	0.8	68.8
		Financial Fraud	0.9	77.4
		Intellectual Property Theft	0.7	60.2
R&D Data	87	Data Breaches	0.8	69.6
		Unauthorized Access	0.6	52.2
		Financial Fraud	0.9	78.3
		Intellectual Property Theft	0.8	69.6
Vendor Data	57	Data Breaches	0.9	51.3
		Unauthorized Access	0.7	39.9
		Financial Fraud	0.9	51.3
		Intellectual Property Theft	0.7	39.9
Contractor Data	74	Data Breaches	0.8	59.2
		Unauthorized Access	0.6	44.4
		Financial Fraud	0.5	37
		Intellectual Property Theft	0.8	59.2

3.3.5 SOFTWARE VRA:

Asset	Asset Impact	Vulnerability	Likelihood	Risk Rating Factor
SensorDrill	100	Software Vulnerabilities	0.5	50
		Code Injection Risks	0.6	60
		Data Leaks	0.8	80
		Malware Injections	0.6	60
		VM Escape Vulnerabilities	0.4	40
		Limited Protection	0.5	50
MeasureMe	100	Software Vulnerabilities	0.6	60
		Code Injection Risks	0.5	50
		Data Leaks	0.8	80
		Malware Injections	0.7	70
		VM Escape Vulnerabilities	0.5	50
		Limited Protection	0.6	60
Shake and Quake	85	Software Vulnerabilities	0.7	59.5
		Code Injection Risks	0.5	42.5
		Data Leaks	0.8	68
		Malware Injections	0.6	51
		VM Escape Vulnerabilities	0.6	51
		Limited Protection	0.7	59.5
Project 2 (In Research and Development)	97	Software Vulnerabilities	0.7	67.9
		Code Injection Risks	0.6	58.2
		Data Leaks	0.8	77.6
		Malware Injections	0.6	58.2

		VM Escape Vulnerabilities	0.5	48.5
		Limited Protection	0.7	67.9
Windows 10 Pro	51	Software Vulnerabilities	0.8	40.8
		Code Injection Risks	0.6	30.6
		Data Leaks	0.9	45.9
		Malware Injections	0.9	45.9
		VM Escape Vulnerabilities	0.7	35.7
		Limited Protection	0.7	35.7
Windows 8.1	51	Software Vulnerabilities	0.8	40.8
		Code Injection Risks	0.6	30.6
		Data Leaks	0.7	35.7
		Malware Injections	0.5	25.5
		VM Escape Vulnerabilities	0.6	30.6
		Limited Protection	0.8	40.8
Windows Server 2016	61	Software Vulnerabilities	0.8	48.8
		Code Injection Risks	0.4	24.4
		Data Leaks	0.7	42.7
		Malware Injections	0.6	36.6
		VM Escape Vulnerabilities	0.6	36.6
		Limited Protection	0.6	36.6
Ubuntu 16.04	10	Software Vulnerabilities	0.8	8
		Code Injection Risks	0.4	8
		Data Leaks	0.8	8
		Malware Injections	0.6	8
		VM Escape Vulnerabilities	0.7	8
		Limited Protection	0.6	8
Red Hat Enterprises	14	Software Vulnerabilities	0.6	8.4

		Code Injection Risks	0.4	5.6
		Data Leaks	0.8	11.2
		Malware Injections	0.6	8.4
		VM Escape Vulnerabilities	0.4	5.6
		Limited Protection	0.7	9.8
Virtual Machines	13	Software Vulnerabilities	0.7	9.1
		Code Injection Risks	0.5	6.5
		Data Leaks	0.8	10.4
		Malware Injections	0.6	7.8
		VM Escape Vulnerabilities	0.5	6.5
		Limited Protection	0.7	9.1
Microsoft Outlook 2016	37	Software Vulnerabilities	0.7	25.9
		Code Injection Risks	0.4	14.8
		Data Leaks	0.8	29.6
		Malware Injections	0.6	22.2
		VM Escape Vulnerabilities	0.6	22.2
		Limited Protection	0.7	25.9
Microsoft Office 2016	19	Software Vulnerabilities	0.8	15.2
		Code Injection Risks	0.8	15.2
		Data Leaks	0.9	17.1
		Malware Injections	0.7	13.3
		VM Escape Vulnerabilities	0.6	11.4
		Limited Protection	0.8	15.2
Symantec Backup Executive	13	Software Vulnerabilities	0.5	6.5
		Code Injection Risks	0.5	6.5
		Data Leaks	0.7	9.1
		Malware Injections	0.6	7.8

		VM Escape Vulnerabilities	0.4	5.2
		Limited Protection	0.7	9.1
McAfee Antivirus	35	Software Vulnerabilities	0.7	24.5
		Code Injection Risks	0.5	17.5
		Data Leaks	0.8	28
		Malware Injections	0.6	21
		VM Escape Vulnerabilities	0.5	17.5
		Limited Protection	0.7	24.5
Xero (Accounting Software)	54	Software Vulnerabilities	0.6	32.4
		Code Injection Risks	0.5	27
		Data Leaks	0.7	37.8
		Malware Injections	0.6	32.4
		VM Escape Vulnerabilities	0.5	27
		Limited Protection	0.7	37.8

3.3.6 PROCEDURE VRA:

Asset	Asset Impact	Vulnerability	Likelihood	Risk Rating Factor
Access Control Procedures	66	Inadequate Procedures	0.8	52.8
		Human Errors	0.7	46.2
		Insecure Data Handling	0.4	26.4
		Unauthorized Access and Data Breach	0.9	59.4
Disaster Recovery Plan	69	Inadequate Procedures	0.5	34.5
		Human Errors	0.6	41.4
		Insecure Data Handling	0.3	20.7
		Unauthorized Access and Data Breach	0.7	48.3
Contractor Onboarding Procedure	40	Inadequate Procedures	0.4	16
		Human Errors	0.6	24
		Insecure Data Handling	0.2	8

		Unauthorized Access and Data Breach	0.5	20
Client Onboarding Procedure	56	Inadequate Procedures	0.3	16.8
		Human Errors	0.5	28
		Insecure Data Handling	0.4	22.4
		Unauthorized Access and Data Breach	0.6	33.6
Vendor Onboarding Procedure	31	Inadequate Procedures	0.2	6.2
		Human Errors	0.4	12.4
		Insecure Data Handling	0.3	9.3
		Unauthorized Access and Data Breach	0.5	15.5
Contractor Offboarding Procedure	33	Inadequate Procedures	0.2	6.6
		Human Errors	0.3	9.9
		Insecure Data Handling	0.1	3.3
		Unauthorized Access and Data Breach	0.4	13.2
Client Offboarding Procedure	26	Inadequate Procedures	0.1	2.6
		Human Errors	0.2	5.2
		Insecure Data Handling	0.1	2.6
		Unauthorized Access and Data Breach	0.3	7.8
Vendor Offboarding Procedure	21	Inadequate Procedures	0.1	2.1
		Human Errors	0.2	4.2
		Insecure Data Handling	0.1	2.1
		Unauthorized Access and Data Breach	0.3	6.3

3.4 THREAT VULNERABILITY ASSESSMENT:

Creating a Threat Vulnerability Assessment (TVA) is the last step in risk assessment. TVA creates a table by combining the lists of assets and threats. The first row of the table has the list of assets, while the first column contains the list of threats.

Colour scheme for Likely-Hood:

0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1	0

3.4.1 PEOPLE TVA:

Threat/Assets	CEO	Chief Security Officer	Chief Information Technology Officer	Director Sales & Product	Division Head - Research and Development	PeopleRus Human Resource Pty Ltd.	Division Head - Service and Technical Support	Division Head - Software	Legal Officer	Middle Management	Division Head - Data Processing	Computex Pty Ltd.	Lower Staff	Clean and Mean Pty Ltd.	Printmaster Pty Ltd.	Hungerbuster Pty Ltd.
Insider threats, unauthorized access	0.9	0.9	0.9	0.8	0.7	0.9	0.7	0.7	0.7	0.7	0.6	0.8	0.6	0.6	0.5	0.2
Intellectual Property Theft	0.9	0.9	0.9	0.7	0.6	0.8	0.6	0.6	0.6	0.6	0.5	0.9	0.5	0.6	0.8	0.2
Identity Theft	0.9	0.9	0.9	0.7	0.6	0.8	0.6	0.6	0.6	0.6	0.5	0.7	0.5	0.6	0.8	0.2
Human Errors	0.9	0.8	0.8	0.5	0.5	0.7	0.5	0.5	0.5	0.5	0.4	0.7	0.4	0.5	0.7	0.1
Social Engineering	0.9	0.8	0.8	0.6	0.5	0.7	0.5	0.5	0.5	0.5	0.4	0.4	0.4	0.5	0.7	0.1
Network Attacks	0.9	0.8	0.8	0.6	0.5	0.4	0.5	0.5	0.5	0.5	0.4	0.3	0.4	0.1	0.4	0.1
Data Breaches	0.8	0.7	0.7	0.4	0.3	0.6	0.3	0.3	0.3	0.3	0.2	0.8	0.2	0.2	0.6	0

3.4.2 DATA TVA:

Threat/Assets	Customer Data	Employee Data	R&D Data	Financial Data	Contractor Data	Vendor Data
Data Breaches	0.9	0.8	0.8	0.9	0.8	0.9
Financial Fraud	0.8	0.6	0.9	0.9	0.5	0.5
Intellectual Property Theft	0.7	0.8	0.8	0.7	0.8	0.8
Unauthorized Access	0.7	0.7	0.6	0.8	0.6	0.6

3.4.3 NETWORKING TVA:

Threat/Assets	Cisco 3750E	Big Lake ISP	Cisco 2960 Access Switch	Cisco 1242AG	Cisco 3845 ISR
Network Attacks	0.7	0.9	0.9	0.8	0.8
Distributed Denial of Service Attacks	0.9	0.8	0.8	0.8	0.8
Unauthorized Access	0.9	0.7	0.8	0.8	0.8
Data Exfiltration	0.8	0.7	0.7	0.7	0.7
Default Credentials	0.6	0.5	0.6	0.5	0.6
Outdated Firmware	0.5	0.4	0.4	0.5	0.4

3.4.4 HARDWARE TVA:

Threat/Assets	IBM Blade Center	Seismic Data Processing Servers	Tape Array	VOIP Servers	Dell Inspiron 15 Laptop	Dell Precision 3590 Workstation	Domain Controller Server	Web Server	HP Proliant Gen9 Servers	Data Backup Tapes	HP 1/8 G2 Tape Autoloader	File and Print Server	Cisco 7941G IP Phone	Konica Minolta C350 MFC
Data Breaches	0.9	0.9	0.8	0.8	0.8	0.9	0.9	0.9	0.8	0.9	0.8	0.9	0.8	0.9
Unauthorized Access	0.8	0.8	0.7	0.9	0.9	0.8	0.9	0.9	0.8	0.9	0.7	0.9	0.7	0.7
Malware Infection	0.7	0.8	0.4	0.9	0.9	0.9	0.8	0.9	0.9	0.8	0.8	0.8	0.9	0.8
Firmware Vulnerabilities	0.7	0.8	0.6	0.8	0.7	0.8	0.8	0.9	0.8	0.9	0.8	0.8	0.7	0.8
Unpactched OS Software	0.7	0.6	0.5	0.8	0.9	0.7	0.7	0.8	0.7	0.7	0.5	0.6	0.6	0.7
Outdated Firmware	0.6	0.6	0.5	0.6	0.7	0.7	0.7	0.7	0.7	0.7	0.7	0.6	0.6	0.6

3.4.5 SOFTWARE TVA:

Threat/Assets	Xero (Accounting Software)	Windows 10 Pro	Windows 8.1	Microsoft Outlook 2016	McAfee Antivirus	Microsoft Office 2016	Red Hat Enterprises	Virtual Machines	Symantec Backup Executive	Ubuntu 16.04
Data Leaks	0.7	0.9	0.7	0.8	0.8	0.9	0.8	0.8	0.7	0.8
Software Vulnerabilities	0.6	0.8	0.8	0.7	0.7	0.8	0.6	0.7	0.5	0.8
Limited Protection	0.7	0.7	0.8	0.7	0.7	0.8	0.7	0.7	0.7	0.6
Malware Injections	0.6	0.9	0.5	0.6	0.6	0.7	0.6	0.6	0.6	0.6
Code Injection Risks	0.5	0.6	0.6	0.4	0.5	0.8	0.4	0.5	0.5	0.4
VM Escape Vulnerabilities	0.5	0.7	0.6	0.6	0.5	0.6	0.4	0.5	0.4	0.7

3.4.6 PROCEDURES TVA:

Threat/Assets	Disaster Recovery Plan	Access Control Procedures	Client Onboarding Procedure	Contractor Onboarding Procedure	Contractor Offboarding Procedure	Vendor Onboarding Procedure	Client Offboarding Procedure	Vendor Offboarding Procedure
Inadequate Procedures	0.5	0.8	0.3	0.4	0.2	0.2	0.1	0.1
Human Errors	0.6	0.7	0.5	0.6	0.3	0.4	0.2	0.2
Insecure Data Handling	0.3	0.4	0.4	0.2	0.1	0.3	0.1	0.1
Unauthorized Access and Data Breach	0.7	0.9	0.6	0.5	0.4	0.5	0.3	0.3

RISK MANAGEMENT:

The goal of risk management is to minimize uncertainty by predicting potential problems and taking appropriate measures to mitigate them(*What Is Risk Management? | APM*, n.d.).

In our risk management and control strategy, we have identified key measures to protect PetroCompass Technologies. Businesses can manage risks through several strategies:

- Risk Transferral: This involves shifting the risk to another party, such as through insurance, outsourcing, or contracts, to reduce the impact or likelihood of a risk affecting the organization.

- Risk Defence: This strategy focuses on preventing risks from materializing by implementing measures such as firewalls, encryption, access controls, and physical security to protect assets.

- Risk Mitigation: Mitigation involves reducing the impact or likelihood of a risk occurring. This can include implementing controls, developing contingency plans, or diversifying resources to lessen the effects of an adverse event.

- Risk Acceptance: This is the decision to acknowledge a risk without taking any specific action to address it. It is often used when the cost of mitigating the risk is higher than the potential impact of the risk itself.

- Risk Avoidance: This strategy involves avoiding activities or situations that could lead to a risk. It may include not pursuing certain opportunities or investments that pose a significant threat to the organization(Yu, 2024).

4.1 PEOPLE:

People - Asset	Mitigation Strategy	Reasoning
Clean and Mean Pty Ltd.	Transferal	Transferring the risk to a third-party vendor through contractual agreements and insurance can help mitigate the risk associated with their services, ensuring that the vendor is responsible for any security breaches or disruptions.
Computex Pty Ltd.	Mitigation	Mitigating the risk by implementing strong contractual agreements and regular reviews of security practices can help ensure that their services meet security standards and minimize the risk of data breaches or disruptions.

Printmaster Pty Ltd.	Avoidance	Avoiding the risk by restricting access to sensitive printing materials and ensuring secure printing practices can help prevent unauthorized access to sensitive documents and reduce the risk of data breaches.
PeopleRus Human Resource Pty Ltd.	Acceptance	Accepting the risk by limiting the amount of personal data shared to only what is necessary can help minimize exposure of personal data and reduce the impact of any potential data breaches.
Hungerbuster Pty Ltd.	Mitigation	Mitigating the risk by ensuring compliance with food safety and hygiene regulations and regularly inspecting their premises can help prevent food-related health risks and minimize the impact of any potential incidents.
Chief Security Officer	Mitigation	Mitigating the risk by regularly reviewing and updating security policies, conducting regular security audits, and providing ongoing training for the CSO and the security team can help ensure that security measures are effective and up-to-date.
CEO	Acceptance	Accepting the risk by acknowledging that the CEO is a high-profile target for cyber attacks and implementing strong security measures such as multi-factor authentication, regular security briefings, and limiting access to sensitive information can help minimize the impact of any potential security breaches.
Chief Information Technology Officer	Avoidance	Avoiding the risk by ensuring that the CITO is aware of and compliant with all relevant data protection regulations, implementing strict access controls and encryption measures, and regularly reviewing security practices can help prevent data breaches and minimize the risk of regulatory fines.
Director Sales & Product	Transferal	Transferring the risk to a third-party vendor through contractual agreements and insurance can help mitigate the risk associated with their services, ensuring that the vendor is responsible for any security breaches or disruptions.

Division Head - Research and Development	Mitigation	Mitigating the risk by implementing strict access controls, encryption measures, and regular security audits can help protect sensitive research and development data and minimize the risk of data breaches.
Division Head - Software	Acceptance	Accepting the risk by acknowledging that the Division Head of Software is a key target for cyber attacks and implementing strong security measures such as regular security briefings, multi-factor authentication, and limiting access to sensitive information can help minimize the impact of any potential security breaches.
Division Head - Data Processing	Mitigation	Mitigating the risk by implementing strict access controls, encryption measures, and regular security audits can help protect sensitive data and minimize the risk of data breaches.
Division Head - Service and Technical Support	Mitigation	Mitigating the risk by ensuring that the Division Head of Service and Technical Support is aware of and compliant with all relevant data protection regulations, implementing strict access controls and encryption measures, and regularly reviewing security practices can help prevent data breaches and minimize the risk of regulatory fines.
Middle Management	Acceptance	Accepting the risk by acknowledging that middle management may not always follow security protocols and implementing regular security training and audits can help mitigate the risk of security breaches caused by human error.
Legal Officer	Avoidance	Avoiding the risk by ensuring that the Legal Officer is aware of and compliant with all relevant data protection regulations, implementing strict access controls and encryption measures, and regularly reviewing security practices can help prevent data breaches and minimize the risk of regulatory fines.
Lower Staff	Mitigation	Mitigating the risk by providing regular security training to lower staff, implementing strict access controls, and conducting regular audits can help

		minimize the risk of security breaches caused by human error or negligence.

4.2 NETWORKING:

Networking - Asset	Mitigation Strategy	Reasoning
Cisco 3750E	Mitigation/Defense	Implementing regular security updates and patches, configuring access control lists (ACLs) to control traffic, and using strong encryption methods (IPSec) can help defend the risk of unauthorized access and network vulnerabilities.
Cisco 3845 ISR	Mitigation	Applying security best practices such as disabling unnecessary services, enabling encryption for sensitive data, and keeping the device firmware up to date can help mitigate the risk of security breaches and unauthorized access to the router.
Cisco 2960 Access Switch	Transferal	The switch vendor has expertise and responsibility for maintaining the device's security. A well-defined Service Level Agreement (SLA) ensures they provide timely updates and address vulnerabilities.
Cisco 1242AG	Defense	Securing the wireless network by using strong encryption, enabling MAC address filtering, and regularly monitoring for unauthorized access can help defend the risk of security breaches and unauthorized use of the wireless network.
Big Lake ISP	Transferal	Ensuring that the ISP follows security best practices, such as implementing firewalls, intrusion detection systems, and encryption protocols, can help mitigate the risk of data breaches and unauthorized access to the network through Big Lake.

4.3 HARDWARE:

Hardware - Asset	Mitigation Strategy	Reasoning
Konica Minolta C350 MFC	Acceptance	Given the relatively low impact and likelihood of security breaches through a printer, accepting the risk may be appropriate, focusing instead on general network security measures.
Cisco 7941G IP Phone	Defense	Disable unused features on the IP phones to reduce the attack surface as IP phones can be targeted for eavesdropping or denial-of-service attacks. Disabling unused features minimizes vulnerabilities and ensuring regular firmware updates patch security holes.
Dell Inspiron 15 Laptop	Mitigation	Implementing full disk encryption, using strong passwords, enabling firewall, and keeping the operating system and software up to date can help mitigate the risk of data theft and unauthorized access to the laptop.
Dell Precision 3590 Workstation	Mitigation	Applying security best practices such as using strong passwords, implementing access control measures, and keeping the operating system and applications up to date can help mitigate the risk of unauthorized access and data breaches.
HP Proliant Gen9 Servers	Mitigation	Implementing access controls, regularly updating firmware and software, using strong authentication methods, and monitoring for suspicious activity can help mitigate the risk of unauthorized access and data breaches on the servers.
HP 1/8 G2 Tape Autoloader	Transferal	Store the backup tapes offsite in a secure facility with a reputable service provider as physical theft of backup tapes can be catastrophic.
Domain Controller Server	Mitigation	Implementing strong authentication methods, regularly updating software, monitoring for unauthorized access, and using network

		segmentation can help mitigate the risk of unauthorized access and data breaches on the domain controller.
File and Print Server	Mitigation	Implementing access controls, regularly updating software, using encryption for sensitive data, and monitoring for unauthorized access can help mitigate the risk of data breaches and unauthorized access to the server.
Web Server	Mitigation	Implementing strong authentication, regular security updates, using secure communication protocols and monitoring for suspicious activity can help mitigate the risk of web server attacks and data breaches.
Data Backup Tapes	Mitigation	Implementing strong physical security measures and encrypting backup data, and regularly auditing tape inventories, can help mitigate the risk of data theft and loss.
Seismic Data Processing Servers	Mitigation	Implementing access controls, regularly updating software, using encryption for sensitive data, and monitoring for unauthorized access can help mitigate the risk of data breaches and unauthorized access to the servers.
IBM Blade Center	Mitigation	Implementing access controls, regularly updating firmware and software, using strong authentication methods, and monitoring for suspicious activity can help mitigate the risk of unauthorized access and data breaches.
VOIP Servers	Defense	Implementing security measures such as encrypting voice traffic, using strong authentication, disabling unused features and services, regularly updating firmware, and monitoring for suspicious activity can help mitigate the risk of unauthorized access and eavesdropping on VOIP communications.
Tape Array	Mitigation	Implementing physical security measures, such as securing the tape array in a locked room or cabinet, monitoring access to the device, and

		regularly auditing tape inventories, can help mitigate the risk of data theft and loss.

4.4 SOFTWARE:

Software - Asset	Mitigation Strategy	Reasoning
SensorDrill	Mitigation	Implementing mitigation measures such as regular updates, security patches, and access controls are necessary to prevent unauthorized access and ensure its reliability.
MeasureMe	Mitigation	MeasureMe requires mitigation strategies to safeguard its functionality and prevent unauthorized access, ensuring the integrity and accuracy of the monitoring data.
Shake and Quake	Mitigation	Mitigating risks associated with Shake and Quake involves implementing robust access controls, encryption, and regular backups to protect sensitive seismic data.
Project 2	Acceptance	Since Project 2 is already in the alpha testing stage and nearing completion, accepting the associated risks while implementing necessary security measures is more practical than avoiding or transferring them.
Windows 10 Pro	Mitigation	Mitigation strategies such as regular security updates, antivirus software, and user awareness training can help mitigate security risks associated with Windows 10 Pro.
Windows 8.1	Mitigation	Mitigation measures are essential for securing Windows 8.1 systems against potential vulnerabilities and cyber threats.
Windows Server 2016	Mitigation	Implementing best security practices, access controls, and regular updates can mitigate risks associated with Windows Server 2016, ensuring the security and stability of server operations.

Ubuntu 16.04	Mitigation	Although Ubuntu is known for its security features, mitigation strategies such as regular updates and proper configuration are still necessary to protect against vulnerabilities and attacks.
Red Hat Enterprises	Mitigation	Red Hat Enterprise Linux also requires regular updates, proper configuration, and access controls to mitigate security risks and ensure the security of the system.
Virtual Machines	Mitigation	Implementing security measures such as network segmentation and regular backups can help mitigate risks associated with virtual machines.
Microsoft Outlook 2016	Mitigation	Since Outlook is commonly targeted by phishing attacks, mitigation strategies such as user training, email filtering, and applying security updates are necessary to reduce the risk of email-based threats.
Microsoft Office 2016	Mitigation	Microsoft Office applications should be regularly updated and protected with antivirus software to mitigate the risk of malware and other security threats.
Symantec Backup Executive	Mitigation	Mitigation measures for Backup Exec include regular updates, secure storage of backup data, and encryption to protect sensitive information from unauthorized access and data loss.
McAfee Antivirus	Mitigation	While antivirus software helps protect against malware, regular updates and monitoring are essential to maintain its effectiveness and mitigate evolving security threats.
Xero (Accounting Software)	Mitigation	Mitigating risks associated with accounting software like Xero involves regular updates, access controls, and secure storage of financial data to prevent unauthorized access and ensure data integrity.

4.5 DATA:

Data - Asset	Mitigation Strategies	Reasoning
Customer Data	Mitigation/Defense	Customer data is sensitive and must be protected from unauthorized access and breaches. Mitigation strategies include encryption and rest and in transit (SSL/TLS), access controls, and regular audits.
Employee Data	Mitigation/Defense	Employee data contains personal and confidential information. Mitigation measures such as access controls, data classification, encryption, disposal of outdated data and regular audits are essential to protect this data.
Financial Data	Mitigation/Defense	Financial data is critical and must be protected from unauthorized access and fraud. Mitigation strategies include strong access controls with multi-factor authentication, encryption, secure storage, and regular audits. Penetration testing should be conducted to find and identify vulnerabilities and security weaknesses.
R&D Data	Mitigation	Research and development data is proprietary and must be protected from theft and unauthorized access. Mitigation measures include data classification, access controls based on project involvement, encryption, and regular audits.
Vendor Data	Mitigation	Vendor data may contain sensitive information and must be protected. Mitigation strategies include secure storage, access controls, and regular audits.
Contractor Data	Mitigation/Transferal	Contractor data may include confidential information and must be protected. Contractors should be required to undergo a security awareness training. Data should be stored securely, access controls systems should be implemented.

4.6 PROCEDURE:

Procedure - Asset	Mitigation Strategies	Reasoning
Access Control Procedures	Acceptance	Access control procedures are necessary for managing and securing access to company resources. Accepting the risk acknowledges that some level of risk is inherent in access control processes, and the organization is willing to manage it without further action.
Disaster Recovery Plan	Mitigation	A disaster recovery plan is critical for ensuring business continuity in the event of a disaster. Mitigation measures include regular testing, backup, and redundancy to minimize the impact of potential disasters.
Contractor Onboarding	Mitigation	Contractor onboarding procedures help ensure that contractors understand and adhere to the organization's security policies and practices. Mitigation measures include background checks and security training.
Client Onboarding	Mitigation	Client onboarding procedures help ensure that clients understand and adhere to the organization's security policies and practices. Mitigation measures include verification of client identity and agreement to security terms.
Vendor Onboarding	Mitigation	Vendor onboarding procedures help ensure that vendors understand and adhere to the organization's security policies and practices. Mitigation measures include vetting vendors and securing contracts.
Contractor Offboarding	Termination	Contractor offboarding procedures help ensure that contractors no longer have access to sensitive information or systems. Former contractors can pose a security risk if they retain access. A defined process including revoking access to all systems and data upon completion of contract and ensuring secure disposal or return of issued equipment is necessary.

Client Offboarding	Mitigation	Client offboarding procedures help ensure that clients no longer have access to sensitive information or systems. Mitigation measures include terminating contracts and revoking access.
Vendor Offboarding	Termination	Vendor offboarding procedures help ensure that vendors no longer have access to sensitive information or systems.

COST-BENEFIT ANALYSIS:

An organization's profitability can be determined by estimating the costs and benefits of investments or initiatives through the use of a cost-benefit analysis (CBA). When making decisions about government policies, projects, and company administration, a CBA is a useful tool. Cost-benefit analysis is a systematic method used to determine the advantages and disadvantages of different project or business proposals(Landau, 2024).

Step one involves determining the asset value (AV) and exposure factor (EF), where EF represents the percentage loss expected during a vulnerability occurrence.

Step two calculates the single loss expectancy (SLE), indicating the potential loss from a single attack using the formula SLE = AV * EF.

Step three computes the Annual Loss Expectancy (ALE), requiring the determination of the Annualized Rate of Occurrence (ARO), which signifies the expected frequency of attacks per year. The formula for ALE is ALE = SLE * ARO.

The final step involves conducting a Cost-Benefit Analysis (CBA), using the ALE values (pre-control and post-control) and the Annual Cost of Safeguard (ACS). The CBA formula is CBA = ALE (pre-control) - ALE (post-control) - ACS.

Variables:

- AV - Asset Value
- EF - Exposure Factor (0 - 1)
- SLE - Single Loss Expectancy (AV x EF)
- Pre/Post ARO - Annual Rate of Occurrence (0 - 100%)
- Pre/Post ALE - Annual Loss Expectancy (SLE x ARO)
- ACS - Annual Cost of Safeguard
- CBA - Cost-Benefit Analysis (Pre ALE - Post ALE - ACS)

5.1 DATA:

Asset	AV	EF	SLE	Pre ARO (%)	Pre ALE	Post ARO (%)	Post ALE	ACS	CBA
Customer Data	$15,000,000	0.6	$9,000,000	25%	$2,250,000	12.50 %	$1,125,000	$1,500,000	$1,125,000
Employee Data	$30,000,000	0.8	$24,000,000	40%	$9,600,000	20%	$6,000,000	$3,000,000	$3,600,000

Financial Data	$20,000,000	0.7	$14,000,000	35%	$4,900,000	17.50%	$2,450,000	$2,500,000	$2,450,000
R&D Data	$18,000,000	0.7	$12,600,000	32.50%	$4,095,000	16.25%	$2,051,250	$2,200,000	$1,843,750
Vendor Data	$32,000,000	0.8	$25,600,000	45%	$11,520,000	22.50%	$5,760,000	$3,200,000	$2,560,000
Contractor Data	$28,000,000	0.8	$22,400,000	42.50%	$9,530,000	21.25%	$4,762,000	$3,000,000	$1,768,000

5.2 PROCEDURES:

Asset	AV	EF	SLE	Pre ARO (%)	Pre ALE	Post ARO (%)	Post ALE	ACS	CBA
Access Control Procedures	$5,000,000	0.5	$2,500,000	20%	$500,000	10%	$250,000	$300,000	$50,000
Disaster Recovery Plan	$8,000,000	0.7	$5,600,000	40%	$2,240,000	20%	$1,120,000	$600,000	$620,000
Contractor Onboarding Procedure	$2,500,000	0.3	$750,000	10%	$75,000	5%	$37,500	$150,000	-$37,500
Client Onboarding Procedure	$3,000,000	0.4	$1,200,000	15%	$180,000	7.50%	$90,000	$200,000	$110,000
Vendor Onboarding Procedure	$3,500,000	0.4	$1,400,000	17.50%	$245,000	8.75%	$122,500	$250,000	$127,500
Contractor Offboarding Procedure	$2,800,000	0.3	$840,000	12%	$100,800	6%	$50,400	$180,000	-$129,600
Client Offboarding Procedure	$3,200,000	0.4	$1,280,000	16%	$204,800	8%	$102,400	$220,000	$117,600
Vendor Offboarding Procedure	$3,600,000	0.4	$1,440,000	18%	$259,200	9%	$129,600	$230,000	$101,400

5.3 PEOPLE:

Asset	AV	EF	SLE	Pre ARO (%)	Pre ALE	Post ARO (%)	Post ALE	ACS	CBA
Clean and Mean Pty Ltd	$5,000,000	0.5	$2,500,000	15%	$375,000	7.50%	$187,500	$300,000	$112,500
Computex Pty Ltd	$2,500,000	0.4	$1,000,000	10%	$100,000	5%	$50,000	$150,000	-$50,000
Printmaster Pty Ltd	$1,500,000	0.3	$450,000	7.50%	$33,750	4%	$18,000	$100,000	-$49,250
PeopleRus Human Resource Pty Ltd	$3,000,000	0.5	$1,500,000	12.50%	$187,500	6.25%	$93,750	$200,000	-$90,250
Hungerbuster Pty Ltd	$1,000,000	0.2	$200,000	5%	$10,000	2.50%	$5,000	$50,000	-$45,000
Chief Security Officer	$50,000,000	0.9	$45,000,000	60%	$27,000,000	30%	$13,500,000	$5,000,000	$8,500,000
Chief Information Technology Officer	$45,000,000	0.9	$40,500,000	55%	$22,275,000	27.50%	$11,137,500	$4,750,000	$6,387,500
Director Sales & Product	$40,000,000	0.9	$36,000,000	50%	$18,000,000	25%	$9,000,000	$4,500,000	$4,500,000
Division Head - Research and Development	$35,000,000	0.9	$31,500,000	45%	$14,175,	22.50%	$7,087,500	$4,400,000	$2,687,500

					000				
Division Head - Software	$33,000,000	0.9	$29,700,000	42.50%	$12,622,500	21.25%	$6,311,250	$4,375,000	$2,936,250
Division Head - Data Processing	$30,000,000	0.9	$27,000,000	40%	$10,800,000	20%	$5,400,000	$4,000,000	$1,400,000
Division Head - Service and Technical Support	$28,000,000	0.9	$25,200,000	37.50%	$9,450,000	18.75%	$4,725,000	$3,750,000	$975,000
Director - Back Office	$36,000,000	0.9	$32,400,000	47.50%	$15,390,000	23.75%	$7,697,500	$4,750,000	$2,947,500
Manager Building and Maintenance	$20,000,000	0.7	$14,000,000	35%	$4,900,000	17.50%	$2,450,000	$2,500,000	$2,450,000
Manager Officer Administration	$18,000,000	0.7	$12,600,000	32.50%	$4,095,000	16.25%	$2,051,250	$2,200,000	$1,843,750
Legal Officer	$7,000,000	0.4	$2,800,000	20%	$560,000	10%	$280,000	$300,000	-$20,000
Staff	$6,000,000	0.4	$2,400,000	18%	$432,000	9%	$216,000	$250,000	-$34,000

5.4 HARDWARE:

Asset	AV	EF	SLE	Pre ARO (%)	Pre ALE	Post ARO (%)	Post ALE	ACS	CBA
Dell Optiplex 360	$800	0.7	$560	20%	$112	5%	$28	$50	$34
Dell Inspiron 15 Laptop	$1,200	0.8	$960	25%	$240	10%	$96	$75	$69
Dell Precision 3590 Workstation	$2,500	0.9	$2,250	30%	$675	15%	$337.50	$150	$187.50
HP Proliant Gen9 Servers	$25,000	0.95	$23,750	40%	$9,500	20%	$4,750	$2,000	$2,750
HP 1/8 G2 Tape Autoloader	$10,000	0.9	$9,000	35%	$3,150	15%	$1,350	$1,000	$800
Domain Controller	$15,000	0.95	$14,250	45%	$6,412.50	25%	$3,562.50	$1,500	$1,350
Printer Server	$5,000	0.8	$4,000	20%	$800	5%	$200	$250	$350
File Server	$12,000	0.95	$11,400	40%	$4,560	20%	$2,280	$1,200	$1,080
Web Server	$8,000	0.9	$7,200	35%	$2,520	15%	$1,080	$800	$640

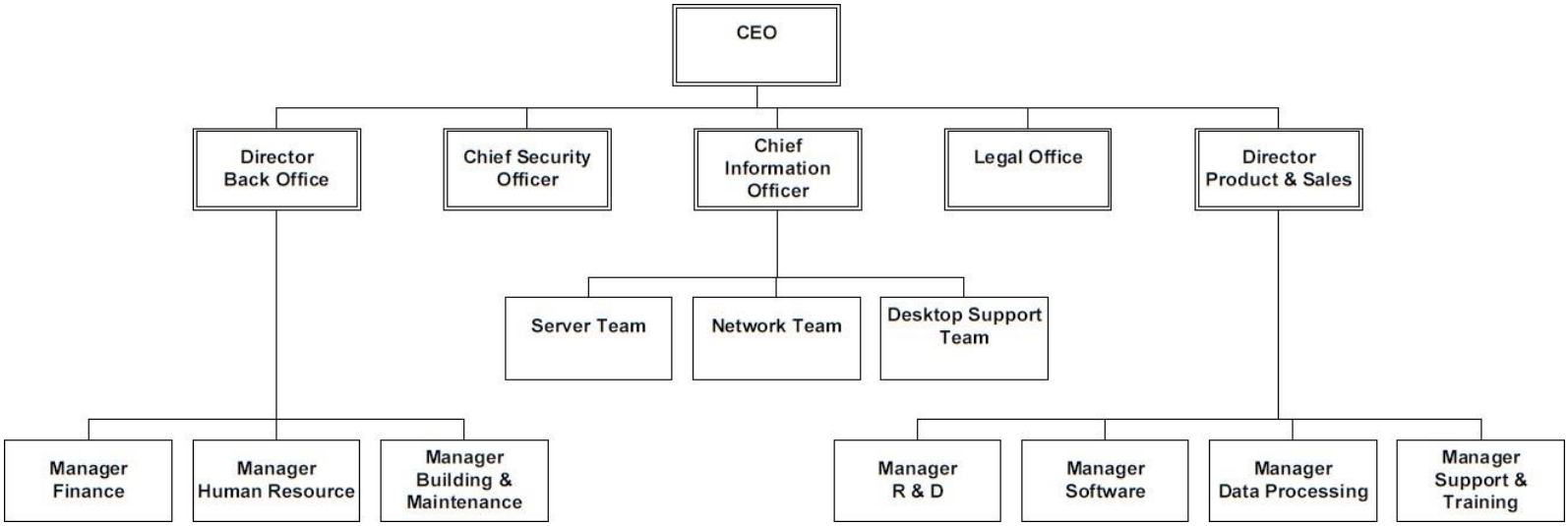
5.5 SOFTWARE:

Asset	AV	EF	SLE	Pre ARO (%)	Pre ALE	Post ARO (%)	Post ALE	ACS	CBA
Sensor Drill	$5,000,000	0.9	$4,500,000	25%	$1,125,000	10%	$450,000	$200,000	$475,000
MeasureMe	$5,000,000	0.9	$4,500,000	25%	$1,125,000	10%	$450,000	$200,000	$475,000
Shake and Quake	$5,000,000	0.9	$4,500,000	25%	$1,125,000	10%	$450,000	$200,000	$475,000
Project 2 (In R&D)	$4,000,000	0.9	$3,600,000	25%	$900,000	10%	$360,000	$150,000	$390,000

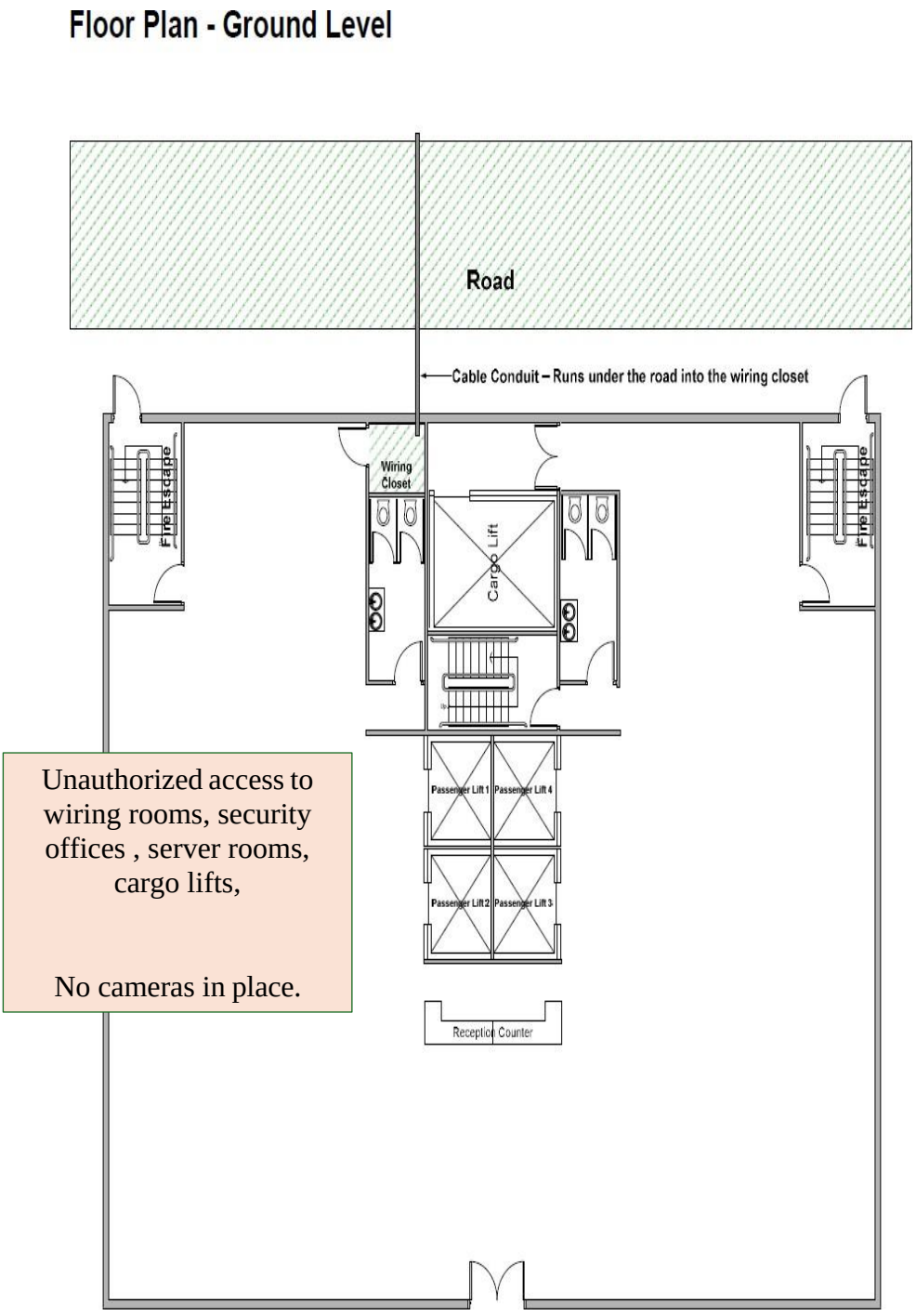
5.6 NETWORKING:

Asset	AV	EF	SLE	Pre ARO (%)	Pre ALE	Post ARO (%)	Post ALE	ACS	CBA
IBM Blade Center	$800,000	0.9	$720,000	30%	$216,000	15%	$108,000	$50,000	$58,000
Cisco 3750E	$100,000	0.8	$80,000	25%	$20,000	10%	$8,000	$10,000	$2,000
Cisco 3845 ISR	$75,000	0.9	$67,500	20%	$13,500	5%	$3,375	$8,000	$2,125
Cisco 2960 Access Switch	$50,000	0.7	$35,000	15%	$5,250	5%	$1,750	$5,000	-$1,500
Cisco 1242AG	$25,000	0.6	$15,000	10%	$1,500	2%	$300	$3,000	-$1,800
Big Lake ISP	$500,000	0.9	$450,000	35%	$157,500	20%	$90,000	$75,000	-$7,500

ORGANIZATION CHART:



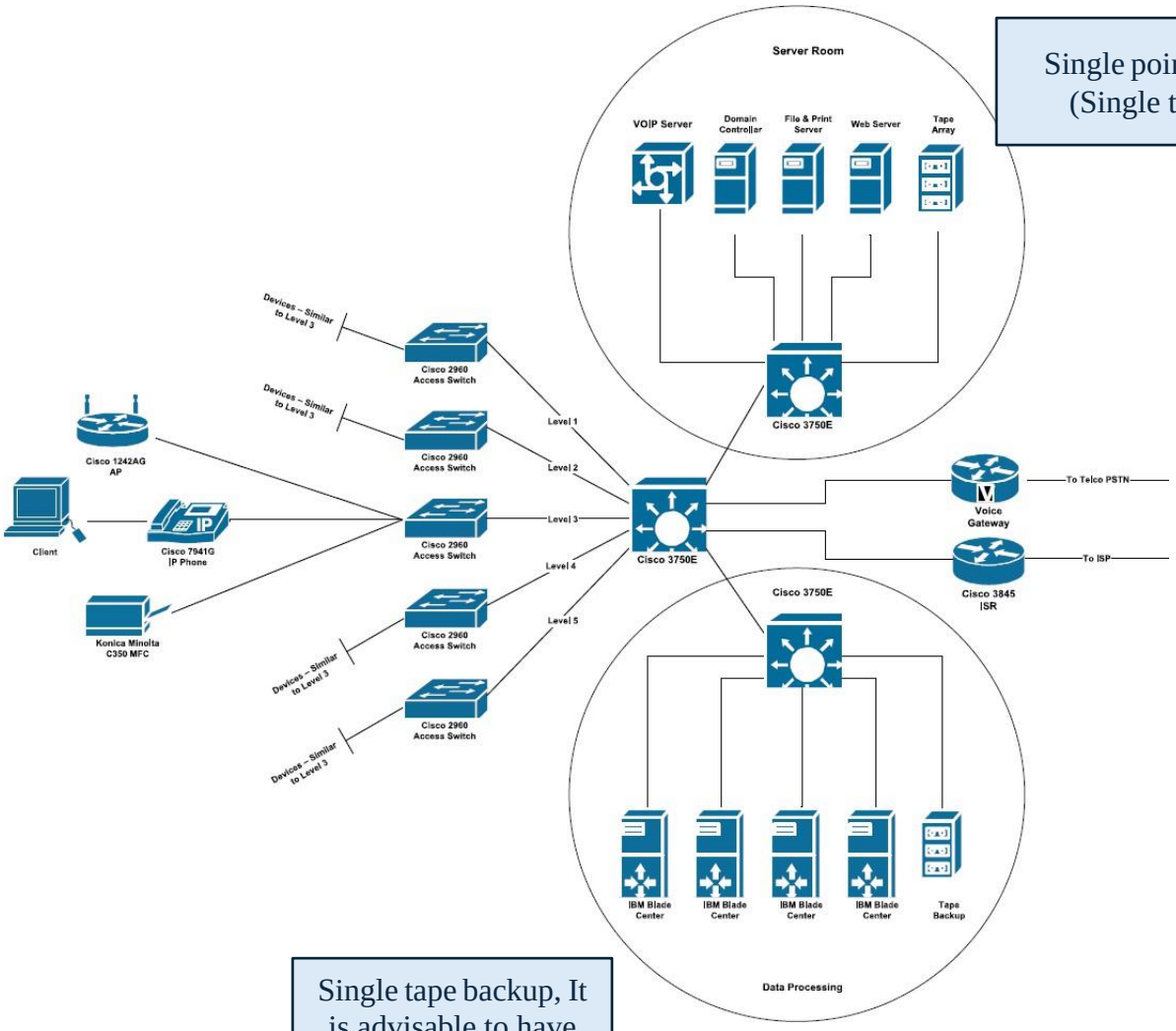
FLOOR PLAN FAULTS:



Unauthorized access to wiring rooms, security offices , server rooms, cargo lifts,

No cameras in place.

NETWORK INFRASTRUCTURE FAULTS:



Single point of failure, (Single tape array)

Single tape backup, It is advisable to have multiples copies of backup. If the only single backup fails that results to loss of data

REFRENCES

Dynatrace. (2024, March 19). *Vulnerability assessment*. Dynatrace. https://www.dynatrace.com/monitoring/platform/application-security/vulnerability-assessment/?utm_source=google&utm_medium=cpc&utm_term=vulnerability%20risk%20management&utm_campaign=me-appsec-application-security&utm_content=none&utm_campaign_id=14569333394&gclsrc=aw.ds&gad_source=1&gclid=Cj0KCQjw5cOwBhCiARIsAJ5njuYrZMFHlRfF_MdKtSivqYYV0A2tPvUixqkR6L_dafISbRdP0DGdwh0aAo7jEALw_wcB

Habte, F. (2022, March 8). *What is Security Management?* Check Point Software. https://www.checkpoint.com/cyber-hub/network-security/what-is-security-management/

Hayes, A. (2024, February 27). *Risk Analysis: Definition, types, limitations, and examples*. Investopedia. https://www.investopedia.com/terms/r/risk-analysis.asp#:~:text=Risk%20analysis%20is%20the%20process,mitigate%20or%20eliminate%20that%20risk

Landau, P. (2024, January 2). *Cost-Benefit Analysis: A Quick Guide with Examples and Templates*. ProjectManager. https://www.projectmanager.com/blog/cost-benefit-analysis-for-projects-a-step-by-step-guide

Risk Assessment | Ready.gov. (n.d.). https://www.ready.gov/business/planning/risk-assessment#:~:text=A%20risk%20assessment%20is%20a,to%20complete%20your%20risk%20assessment

Understanding the NIST cybersecurity framework. (2022, October 6). Federal Trade Commission. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

What is risk management? | APM. (n.d.). https://www.apm.org.uk/resources/what-is-project-management/what-is-risk-management/

What is Weighted Scoring? | craft.io. (2023, April 12). Best Product Management Software | craft.io. https://craft.io/crf_glossary/what-is-weighted-scoring/#:~:text=Weighted%20scoring%20is%20a%20method,on%20a%20set%20of%20criteria

Yasar, K., & Rosencrance, L. (2023, August 21). *risk analysis*. Security. https://www.techtarget.com/searchsecurity/definition/risk-analysis

Yu, J. (2024, February 27). *5 Basic methods for risk management*. Investopedia. https://www.investopedia.com/articles/investing-strategy/082816/methods-handling-risk-quick-guide.asp