Lavanya Sajwan
300381661

Assignment One

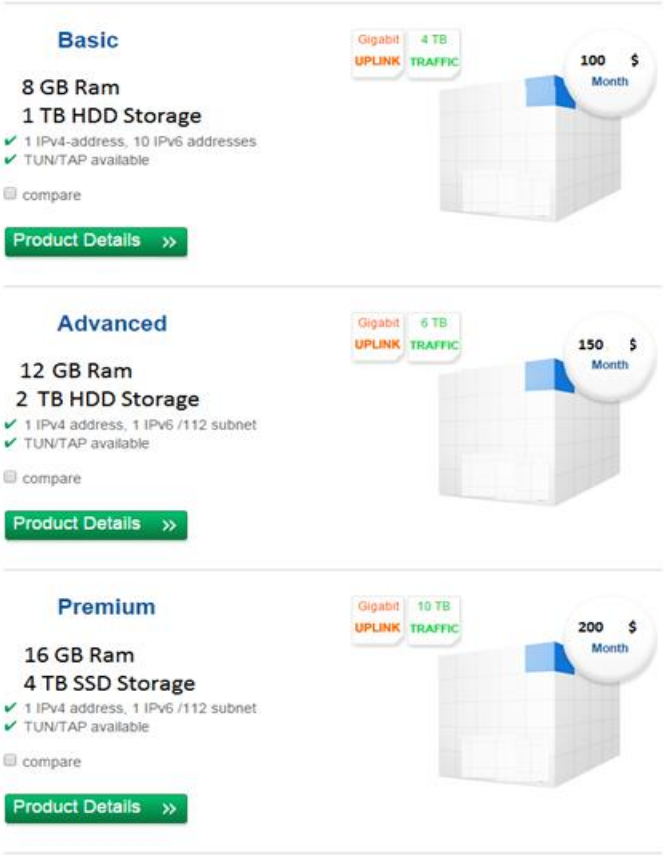
1. Introduction

This document provides a case study on the risk management process. The initial step will cover the risk identification which involves identifying inventory assets, classification and prioritising of assets and threats. The next as a part of this process will be the risk assessment where identification of vulnerabilities will occur as well as identifying and quantifying asset exposure. The final step is the risk control process which will be justifying the current and proposed strategies and controls for each vulnerability and threat.

1.1 Overview

HostNZ is a datacentre that provides Virtual Shared and dedicated Private Servers (VPS) to consumers within New Zealand. The company provides three different hosting plans; the basic, advanced and premium. A comparison is shown in Figure 1 and pricing is in New Zealand dollars.

Figure 1: HostNZ Services



The organisational structure of the company is small with the only primary staff being one Chief Executive Officer (CEO) and three onsite Engineers. The CEO manages the business and is responsible of day-to-day activities, issuing access cards, managing financial data and the hiring and termination of employees. The engineers offer 24/7 support through 8-hour rotational shifts. They have full access to user account information. Tasks involving this information can include registrations of new users, activations and deactivations of user accounts, deletion of account and data recovery system maintenance and password resets. Engineers also ensure that all hardware components are working correctly.

Data handling and consequently destruction is a key aspect of the services that the company provides. Insecure handling of data, or improper data destruction can lead to user data being accessible to third parties outside of the relevant stakeholder (CEO), employees (engineers) and consumers (purchasers of the services). It can also lead to complete loss of data. Both outcomes lead to decrease in public views on the services reliability. This in turn can have negative economic effects on the company.

2. Roles definition and responsibilities

Role	Description and responsibilities
Chief Executive Officer (CEO)	Data Centre Authority responsible for all day-to-day management decisions and activities. Other duties include: – Issuing access cards – Managing financial data – Hiring and termination of employees
Engineers	There are 3 engineers who provide 24/7 support to customers through 8-hours shifts. Engineers have full access to the user account information. The list of their privileges includes: – Registering new users – Activating or deactivating user accounts – Deleting use accounts and data – Data Recovery – System maintenance and upgrades – Password reset Engineers are also responsible for ensuring all hardware components work properly, manage electrical systems within the datacentre, wiring, cooling systems etc.
External Contractors	Responsible for all office-related maintenance (eg. Plumbing, cleaning). Temporary access is provided when needed.

3. Rating and classification definitions

CIA Triad

CIA Triad	Requirements
Confidentiality	Ensures that data is only viewed only by authorised parties.
Integrity	Ensures the accuracy and completeness of services, data and data processing methods.
Availability	Ensures that authorised users have timely and reliable access to services and data.

Value

Value	Description
Confidential	Used for the most sensitive corporate information that must be tightly controlled, even within the organisation. This information must be securely stored and accessed only by authorised personnel. Highly sensitive data intended for specific use or group of individuals with a legitimate need-to-know.
Private/Internal	Used for Information that can be viewed by internal employees, authorised contractors and third parties. It requires less level of protection than Confidential.
External	Used for information that has been approved for public release or use. It requires proportionately less protection than Confidential and Private/Internal.

Likelihood

Likelihood	Description
Certain	It is easy for a threat to exploit the vulnerability without any specialist skills or extra resources [1].
Highly probable	It is feasible for a threat to exploit the vulnerability with minimal skills or extra resources [1].
Possible	It is feasible for a threat to exploit the vulnerability with moderate skills or resources [1].
Possible but unlikely	It is feasible for a threat to exploit the vulnerability but would require significant skills or resources for a threat to exploit the vulnerability [1].
Almost never	It is difficult for a threat to exploit the vulnerability [1].

Impact/Severity

Impact	Description
Severe	There is severe economic loss. Legal liabilities and/or breach of service level agreements. There is severe loss of corporate or public image. Communications and recovery must be shared with customers. Severe ongoing impact on service delivery. Impact cannot be managed without significant extra costs, third-party mitigation (lawyers, marketing etc) and re-planning of business goals and organisational re-structuring. Loss of life
Significant	There is significant economic loss. Some legal liabilities and/or breach of service level agreements. There is significant loss of corporate or public image. Communications and recovery are shared with the customers. Ongoing impact on service delivery. Impact cannot be managed without extra costs and third-party mitigation (lawyers, marketing etc) and re-planning. Some organisational re-structuring may have to occur. Harm to life
Moderate	Limited economic loss. Limited legal liabilities and/or breach of service level agreements. Limited loss of corporate or public image. Communications and recovery may be shared with the customers. Limited impact on service delivery. Impact can be managed with re-planning and limited extra costs and third-party mitigation (lawyers, marketing etc). Injuries
Minor	Minor economic loss. Minor loss of corporate or public image. Communications internally may be needed. Minor impact on service delivery. Impact can be managed with no extra costs and third-party mitigation, with the potential of re-planning.
Minimal	No economic loss. No loss of corporate or public image. No communications internally needed. No impact on service deliver. Impacts can be handled BAU (Business As Usual)

Valuation Criteria

Impact	Description
High	It will result in high financial impacts; loss of assets; loss of reputation with customers and within the corporate business area; major impacts to service delivery; or large legal ramifications.
Medium	It will result in some financial impacts; loss of some assets; some impact to service delivery; or some legal ramifications.
Low	It will result in low financial impacts; low loss of assets; or minor impacts to service delivery.

Asset Categories

Asset Category	Description
Employees	The member of staff at the company.
Procedures	IT actions and standard business of completing tasks and operations.
Data	User details, transactional information, intellectual property, hardcopy, processing and storage, databases and backup files,
Software	Standard business applications, operating systems and security components
Hardware	Systems and peripherals, security devices, networking components and equipment, safety devices
Infrastructure	Components required to manage and safe-keep the datacentre environment.

4. Asset Identification, Categorisation and Classification

An asset is any employee, procedure, data, software, hardware or infrastructure that directly provides value to the company.

4.1 Information asset classification

People Assets

Item ID	Asset Category	Asset Name	Asset Description/Attribute
001	Employees	CEO	Role: CEO Function: Responsible for all day-to-day management decisions and activities.
002	Employees	Engineer	Role: Engineer Function: Responsible for customer support and data/hardware maintenance.

Procedures Assets

Item ID	Asset Category	Asset Name	Asset Description/Attribute
003	Procedures	Personal Use of Devices Policy	Policy: Engineers are advised to avoid using their own laptop/device to perform daily tasks. Intended purpose: To protect HostNZ's assets against virus or malicious software; and to maintain confidentiality and integrity of information.
004	Procedures	Customer Purchases Policy	Policy: All purchases of datacentre services are done online through their purchase system. HostNZ does not allow counter sales of their service. Intended purpose: To protect the integrity of the software licenses sold and so

				that activation of services can occur when payment has been processed and validated to avoid any loss of income.
005	Procedures	Database backup Policy	Policy: Intended purpose:	All transactional data must be cold backed up from the Oracle Database. To protect the integrity of the organisation in case of any disputes. It also allows for availability of information in case of local data loss.
006	Procedures	Saving backup files Policy	Policy: Intended purpose:	Backed up files must be externally saved on a drive. To protect the integrity of the organisation in case of any disputes. It also allows for long-term availability of information in case of local data loss.
007	Procedures	Locking external drive Policy	Policy: Intended purpose:	External drive must be in a locked cupboard in the CEO's office. Protects the confidentiality of data. Also protects the integrity of the organisation in case of any disputes. It also allows for long-term availability of information in case of local data loss.
008	Procedures	Customers login Policy	Policy: Intended purpose:	Customers log into a unique system (1**, 209.50.1) using SSH service. Each customer has their own unique system which differentiates from others. This overall, protects the confidentiality, integrity and availability of data.
009	Procedures	Customer Reset and	Policy:	Once logged in, customers must enter their VPS management system details to

		Deletion of Data Policy		reset their VPS to initial state. All customer data is deleted in the process. Customers can also call HostNZ or email to request a reset. They must supply their personal service information to do so. Intended purpose: To give the opportunity to restart and protects from unwanted deletion. This overall, protects the confidentiality, integrity and availability of data.
010	Procedures	Cancellation of Service Policy	Policy: Intended purpose:	Customers must email the cancellation form to HostNZ with their personal service information included in order to cancel their service. User account and data are deleted 72 hours after submission of the application. To protect from unwanted deletion and removal of data. This overall, protects the confidentiality, integrity and availability of data.
011	Procedures	Employment documents and transactional data Policy	Policy: Intended purpose:	Employment documents and transactional data must be kept in a safe in the CEO's office. To protect HostNZ's assets against threat actors; and to maintain confidentiality and integrity of information.
012	Procedures	Wireless Access Policy	Policy: Intended purpose:	Employees are not provided with wireless access To protect HostNZ's assets against virus or malicious software; and to maintain confidentiality and integrity of information.
013	Procedures	Physical access for staff Policy	Policy:	Physical access to the datacentre is approved by the

				CEO by the use of access cards. Staff access cards expire every 18 months.
			Intended purpose:	To protect HostNZ's assets against threat actors; and to maintain confidentiality and integrity of information.
014	Procedures	Fire Safety Policy	Policy:	In an event of a fire, staff in the building must exit from their nearest emergency exit and leave all their belongings behind. They must meet in the dedicated assembly area.
			Intended purpose:	To protect HostNZ's employee assets.
015	Procedures	CCTV Security Surveillance 24/7 Policy	Policy:	CCTV cameras record and keep the video for 3 days. The data is then rewritten.
			Intended purpose:	To help with detection of threat actors; and to maintain confidentiality and integrity of information.
016	Procedures	Physical access for external contractors Policy	Policy:	Physical access to the datacentre for any contractors is approved by the CEO. Contractors receive temporary access cards.
			Intended purpose:	To protect HostNZ's assets against threat actors; and to maintain confidentiality and integrity of information.
017	Procedures	Device passwords Policy	Policy:	Engineers are advised to use strong passwords for devices.
			Intended purpose:	To protect HostNZ's assets against virus or malicious software; and to maintain confidentiality and integrity of information.
018	Procedures	Personal staff allocation Policy	Policy:	Staff have their own desk, chair, filing cabinet and basic stationary.

			Intended purpose: To protect HostNZ's assets against threat actors; and to maintain confidentiality, availability and integrity of information.
019	Procedures	Customer ownership Policy	Policy: Customers own any software installed and are responsible for software licenses. Customers own any data stored and are responsible of the content. Intended purpose: To protect HostNZ's against any legal liabilities.

Data Assets

Item ID	Asset Category	Asset Name	Asset Description/Attribute	Classification
020	Data	Customer account information	Description: Detailed information about each current and previous customer (users, services, usage, credentials). Owner: HostNZ	Confidential
021	Data	Transactional data	Description: All information about the types of the services the customers have purchased (including customer information, service information, date of purchase, amount paid). Owner: HostNZ	Confidential
022	Data	Backup files of Database	Description: Cold backup of the Oracle Database (holds transactional data) which occurs every Friday at 11:50PM. Owner: HostNZ	Confidential
023	Data	Service Information (Website)	Description: Information displayed on the website about a service: Basic, Advanced, Premium and sub information (amount of ram, storage etc) Owner: HostNZ	Public

024	Data	User login details	Description: Information used to login to the VPS services; username, password and VPS management system IP address. Owner: HostNZ/Customer	Private
025	Data	Employment Documents	Description: Information about employee contracts; application details; payroll etc. Owner: HostNZ	Confidential
026	Data	CCTV Security Surveillance Recordings	Description: Video recorded activities within the datacenter compound. Owner: HostNZ	Confidential
027	Data	Software licenses	Description: Legally binding guideline for the use of services [2]. Owner: Customer	Private
028	Data	Customer data	Description: Information kept on customer virtual machines. Owner: Customer	Private
029	Data	VPS system information	Description: information about the type of service purchased. Owner: HostNZ	Private
030	Data	Webserver backup files	Description: Backed up website files and information. Owner: HostNZ	Confidential

Software Assets

Item ID	Asset Category	Asset Name	Asset Description/Attribute	
031	Software	Firewall	Description:	Network security system that controls incoming and outgoing network traffic based on a set of rules.
032	Software	Oracle Database	Description:	Database that stores transactional data.
033	Software	Email	Description:	A means to communicate with customers.

034	Software	Debian 7 Linux distribution	Description:	Default operating system on all dedicated PC's.
035	Software	Hypervisor	Description:	Creates and runs virtual machines.
036	Software	CCTV Security Surveillance Software	Description:	Allows for video recordings to occur and get deleted after 3 days.
037	Software	Customer Management Software	Description:	Manages the customer numbers and services associated with them.
038	Software	OpenOffice	Description:	Open-source software for "word processing, spreadsheets, present ations, graphics, databases and more" [3].
039	Software	Snort intrusion detection system	Description:	Open-source network intrusion detection system [4].
040	Software	SSH service	Description:	A network protocol for operating network services securely.
041	Software	VPS Management System	Description:	Manages the Virtual shared and dedicated Private Servers (VPS).
042	Software	Web/Applicatio n Server	Description:	Server which hosts the website and applications.
043	Software	Bastion host	Description:	A server which provides access to a private network from a public network [5].
044	Software	Purchase System	Description:	All purchases of datacentre services occur via this system on the website.
045	Software	Card Access Software	Description:	Software which allows for the card reading to occur and consequent access to different parts of the datacentre.
046	Software	Server	Description:	The dedicated servers that support the virtual servers.

047	Software	Virtual Servers	Description:	The virtual servers whose environments the customers have access to.
048	Software	Intelligent Airflow	Description:	Directs cooler air to areas of higher temperature.

Hardware Assets

Item ID	Asset Category	Asset Name	Asset Description/Attribute	
042	Hardware	Web/application server	Description: Quantity: Category: Location:	Dedicated server for website hosting 1 Systems and peripherals HostNZ premises
046	Hardware	Server	Description: Quantity: Category: Location:	High density heat and dedicated servers. 53 Systems and peripherals HostNZ premises
049	Hardware	24 port Switches	Description: Quantity: Category: Location:	Connects devices on a network. 11 Network components and equipment HostNZ premises
050	Hardware	Routers	Description: Quantity: Category: Location:	Forwards data packets to different parts of a network. 3 Network components and equipment HostNZ premises
051	Hardware	Primary data cabling	Description: Quantity: Category: Location:	Provides a 10gbps primary link to a network provider. - Network components and equipment HostNZ premises
052	Hardware	Secondary data cabling	Description: Quantity:	Provides a 1gbps primary link to a network provider. -

			Category: Location:	Network components and equipment HostNZ premises
053	Hardware	Air conditioning systems	Description: Quantity: Category: Location:	Maintains the temperature of the servers. 6 Safety devices HostNZ premises
054	Hardware	CCTV	Description: Quantity: Category: Location:	Detection system in case of any action by a threat actor. 3 Security devices HostNZ premises
055	Hardware	Smoke Detectors	Description: Quantity: Category: Location:	Alerts staff in case of a fire. 4 Safety devices HostNZ premises
056	Hardware	Fire Extinguishers	Description: Quantity: Category: Location:	Provides a means of extinguishing a small fire. 10 Safety devices HostNZ premises
057	Hardware	Power Distribution Module	Description: Quantity: Category: Location:	Switches power to different parts of the data servers. 2 Systems and peripherals HostNZ premises
058	Hardware	PC's	Description: Quantity: Category: Location:	Dedicated PC's used by staff. 4 Systems and peripherals HostNZ premises
059	Hardware	Access Cards	Description: Quantity: Category: Location:	Provdes access to areas of the datacentre. 4 always, x amount temporary Systems and peripherals, security devices HostNZ premises
060	Hardware	Local Storage	Description: Quantity:	Local system where data is stored. 1

			Category: Location:	Systems and peripherals HostNZ premises
061	Hardware	Key	Description: Quantity: Category: Location:	To access locked drawer of sensitive information 4 Security devices HostNZ premises
062	Hardware	Safe	Description: Quantity: Category: Location:	To store confidential documents 1 Security devices HostNZ premises

Infrastructure Assets

Item ID	Asset Category	Asset Name	Asset Description/Attribute	
053	Infrastructure	Air conditioning systems	Description: Category: Quantity: Location:	System for controlling the humidity, ventilation, and temperature in the building Protection device 6 units Server rooms
054	Infrastructure	CCTV	Description: Category: Quantity: Location:	System for video recording activities within the datacentre. Detective device 3 units Server rooms, hallway, breakroom
055	Infrastructure	Smoke Detectors	Description: Category: Quantity: Location:	System smoke detection in case of a fire. Protection device 4 units Spread across the data centre floor
056	Infrastructure	Fire Extinguishers	Description: Category: Quantity: Location:	Class-E fire extinguishers which provide a means of extinguishing small fires. Protection device 10 units Spread across data centre floor

057	Infrastructure	Power Distribution Module	Description: Category: Quantity: Location:	Switches power to different parts of the data servers. Protection device 2 units Server rooms
063	Infrastructure	Access Card System	Description: Category: Quantity: Location:	System for allowing access to different areas of the building Protection device, Detective device At every door At every door

4.2 Information Asset Valuation

Item ID	Asset Name	Loss of Confidentiality	Loss of Integrity	Loss of Availability
001	CEO	Medium	Medium	Medium
002	Engineer	Medium	Low	Medium
003	Personal Use of Devices Policy	Medium	Medium	Medium
004	Customer Purchases Policy	Low	Low	Low
005	Database backup Policy	High	Low	Medium
006	Saving backup files Policy	Medium	Low	Medium
007	Locking external drive Policy	Medium	Low	Medium
008	Customers login Policy	Low	Low	Low
009	Customer Reset and Deletion of Data Policy	Low	Low	Low
010	Cancellation of Service Policy	Low	Low	Medium
011	Employment documents and transactional data Policy	High	Low	Low
012	Wireless Access Policy	Medium	Medium	Medium
013	Physical access for staff Policy	Medium	Medium	Low
014	Fire Safety Policy	High	High	High
015	CCTV Security Surveillance 24/7 Policy	Low	Low	Low
016	Physical access for external contractors Policy	Medium	Medium	Medium

017	Device passwords Policy	High	High	High
018	Personal staff allocation Policy	Low	Low	Low
019	Customer ownership Policy	Low	Low	Medium
020	Customer account information	Medium	Low	Low
021	Transactional data	Low	Low	Low
022	Backup files of Database	High	High	Medium
023	Service Information (Website)	Low	High	High
024	User login details	High	High	High
025	Employment Documents	High	High	Low
026	CCTV Security Surveillance Recordings	Medium	Medium	Low
027	Software licenses	Medium	High	Low
028	Customer data	Medium	Medium	Medium
029	VPS system information	Medium	Medium	Medium
030	Webserver backup files	Low	Low	Medium
031	Firewall	High	High	High
032	Oracle Database	High	High	High
033	Email	High	High	High
034	Debian 7 Linux distribution	Low to Medium	Low to Medium	Medium
035	Hypervisor	Low to Medium	Medium	High
036	CCTV Security Surveillance Software	Low	Medium	High
037	Customer Management Software	High	High	High
038	OpenOffice	Low to Medium	Low to Medium	Medium
039	Snort intrusion detection system	Low	Medium	Medium
040	SSH service	Medium to High	High	High
041	VPS Management System	Medium	High	High
042	Web/Application Server	Medium	High	High
043	Bastion host	Medium	High	Medium
044	Purchase System	High	High	High
045	Card Access Software	High	High	High

046	Server	High	High	High
047	Virtual Servers	High	High	High
048	Intelligent Airflow	High	High	High
049	24 port Switches	High	High	Medium
050	Routers	High	High	High
051	Primary data cabling	High	High	High
052	Secondary data cabling	Medium	Medium	Medium
053	Air conditioning systems	High	High	High
054	CCTV	Medium to High	High	High
055	Smoke Detectors	High	High	High
056	Fire Extinguishers	High	High	High
057	Power Distribution Module	High	High	High
058	PC's	High	High	High
059	Access Cards	High	High	High
060	Local Storage	Low to Medium	Medium	Medium
061	Key	High	High	High
062	Safe	High	High	High
064	Access Card System	High	High	High

4.3 Information Asset Prioritisation

Key for Valuation Criteria (steps: 0.1)

Low	Medium	High
0.1 - 0.4	0.5 - 0.7	0.8 - 1.0

Item ID	Asset Name	Criterion 1: Impact to time	Criterion 2: Impact to profitability	Criterion 3: Impact to public image	Weighted score
Criteria weights must total 100		30	40	30	
001	CEO	0.9 - will be hard to find a replacement with	0.8	0.9	86

		the specific skill set			
002	Engineer	0.8 – will be hard to find engineers with the specific skill set	0.5	0.5	59
003	Personal Use of Devices Policy	0.5	0.4	0.4	47
004	Customer Purchases Policy	0.7	0.7	0.7	70
005	Database backup Policy	0.4	0.3	0.2	30
006	Saving backup files Policy	0.4	0.3	0.2	30
007	Locking external drive Policy	0.2	0.2	0.1	17
008	Customers login Policy	0.8	0.8	0.8	80
009	Customer Reset and Deletion of Data Policy	0.8	0.6	0.7	69
010	Cancellation of Service Policy	0.7	0.6	0.7	66
011	Employment documents and transactional data Policy	0.6	1.0	1.0	88
012	Wireless Access Policy	0.3	0.4	0.5	40
013	Physical access for staff Policy	0.8	0.6	0.5	63
014	Fire Safety Policy	0.7	0.8	0.4	65
015	CCTV Security Surveillance 24/7 Policy	0.6	0.6	0.6	60
016	Physical access for external contractors Policy	0.8	0.6	0.8	72
017	Device passwords Policy	0.3	0.7	0.8	61
018	Personal staff allocation Policy	0.3	0.1	0.1	16

019	Customer ownership Policy	0.7	0.8	0.9	80
020	Customer account information	1.0	1.0	1.0	100
021	Transactional data	0.8	0.8	0.9	83
022	Backup files of Database	0.4	0.4	0.3	37
023	Service Information (Website)	0.8	0.8	0.6	74
024	User login details	1.0	1.0	1.0	100
025	Employment Documents	0.8	0.7	0.7	73
026	CCTV Security Surveillance Recordings	0.5	0.2	0.3	35
027	Software licenses	0.8	0.7	0.9	79
028	Customer data	0.9	0.9	1.0	93
029	VPS system information	0.2	0.2	0.2	20
030	Webserver backup files	0.1	0.1	0.1	10
031	Firewall	0.9	0.6	0.7	72
032	Oracle Database	0.7	0.7	0.7	70
033	Email	1.0	0.8	0.9	89
034	Debian 7 Linux distribution	0.3	0.2	0.1	20
035	Hypervisor	1.0	0.9	0.8	90
036	CCTV Security Surveillance Software	0.6	0.2	0.2	32
037	Customer Management Software	0.9	0.9	0.9	90
038	OpenOffice	0.1	0.1	0.1	10
039	Snort intrusion detection system	0.8 – no other alternatives that HostNZ uses	0.4	0.5	55
040	SSH service	1.0	1.0	1.0	100 – main point of connection that

					customers use.
041	VPS Management System	0.7	0.6	0.5	60
042	Web/Application Server	0.6	0.6	0.6	60
043	Bastion host	0.6	0.6	0.6	60
044	Purchase System	0.9	1.0	0.9	94
045	Card Access Software	1.0	0.2	0.5	53
046	Server	0.9	0.9	0.9	90
047	Virtual Servers	1.0	1.0	1.0 – and individual virtual server for a customer	100
048	Intelligent Airflow	1.0 – servers can overheat	0.7	0.7	79
049	24 port Switches	0.4	0.4	0.4	40
050	Routers	1.0	0.7	0.6	76
051	Primary data cabling	0.6	0.4	0.2	40
052	Secondary data cabling	0.3	0.3	0.1	24
053	Air conditioning systems	1.0	0.7	0.7	79
054	CCTV	0.8	0.1	0.1	31
055	Smoke Detectors	0.2	0.1	0.1	13
056	Fire Extinguishers	0.1	0.1	0.1	10
057	Power Distribution Module	0.7	0.2	0.2	35
058	PC’s	0.4	0.4	0.4	40
059	Access Cards	0.6	0.1	0.1	25
060	Local Storage	0.1	0.1	0.1	10
061	Key	0.9	0.2	0.1	38
062	Safe	0.9	0.2	0.2	41
063	Access Card System	0.9	0.1	0.1	34

5. Threats and Vulnerabilities

Threats are anyone or anything that can intentionally or unintentionally exploit a vulnerability to manipulate company assets in any way. Vulnerabilities are exposures that can lead to a threat being realised; a weakness in a system.

Threat Categories

Category	Description
Deliberate Threat	Acts that occur on purpose and occur out of malignant intent.
Accidental Threat	Acts that occur by mistake and typically do not occur out of malignant intent.
Technical Failures	When components behave in an unexpected way.
Natural Disaster	Occurrence is due to unexpected natural forces.

Key for Likelihood (Steps: 0.1)

Almost Never	Possible but unlikely	Possible	Highly Probable	Certain
0.1-0.2	0.3-0.4	0.5-0.6	0.7-0.8	0.9-1.0

5.1 Threat Likelihood and Severity

Threat	Likelihood	Severity
Deliberate Threat Theft and fraud	0.6	Significant
Technical Failures Hardware Failures or Errors	0.7	Severe
Technical Failures Software Failures or Errors	0.6	Severe
Natural Disaster Forces of nature	0.3	Significant
Deliberate Threat Espionage or trespass	0.5	Moderate
Accidental Threat Human Error or Failure	0.9	Moderate

Deliberate Threat Information Extortion	0.7	Significant
Deliberate/ Accidental Threat Missing, Inadequate or incomplete controls	0.9	Minor
Accidental Threat Missing, Inadequate or incomplete organisational policy or planning	1.0	Minor
Technical Failures Quality of service deviations between different providers	0.8	Minimal
Deliberate Threat Sabotage or Vandalism	0.6	Moderate
Deliberate Threat Software Attacks	0.8	Significant
Deliberate/ Accidental Threat Technological Obsolesce	0.7	Moderate
Deliberate/ Accidental Threat Fire	0.3	Severe
Accidental Threat Data Breach	0.4	Severe

5.2 Threats and Vulnerability Assessment

Asset IDs	Information Asset Type	Threat	Vulnerability
020, 021, 022, 023, 024, 025, 026, 027, 028, 030, 042, 046, 050, 053, 054, 055, 056, 058, 059, 061,	Data, Hardware	**Deliberate Threat** Theft and fraud	– Lax physical security controls. – Disgruntled employee or contractor. – Lax recruiting processes. – External agents have access to the data centre. – Minimum monitoring is done while external agents are present within the premise – Lack of security education and training – Minimum monitoring of systems and networks – Routers have inadequate security mechanisms in place
042, 046, 049, 050, 051, 052, 053, 054, 055,	Hardware	**Technical Failures** Hardware Failures or Errors	– Lack of backup generators – Potentially faulty equipment – Lack of maintenance – Staff lacking adequate knowledge

056, 057, 058, 059, 060			– Power not distributed adequately – Incorrect temperature – Lack of failsafe in the event of a fire or natural event.
031, 032, 033, 034, 035, 036, 037, 038, 039, 040, 041, 042, 043, 044, 045, 046, 047, 048	Software	**Technical Failures** Software Failures or Errors	– Lack of maintenance – Staff lacking adequate knowledge – Using discontinued or outdated software and packages – Untested or minimally tested, released software
042, 046, 049, 050, 051, 052, 053, 054, 055, 056, 057, 058, 059, 060, 061, 062, 063	Hardware, Infrastructure	**Natural Disaster** Forces of nature	– Lack of backup generators – Suitable controls not provided
020, 021, 022, 023, 024, 025, 026, 027, 028, 029, 030, 031, 032, 033, 034, 035, 036, 037, 038, 039, 040, 041, 042, 043, 044, 045, 046, 047, 048	Data, Software	**Deliberate Threat** Espionage or trespass	– Lax physical security controls. – Lax virtual security controls. – Disgruntled employee or contractor. – Lax recruiting processes. – External agents have access to the data centre. – Minimum monitoring is done while external agents are present within the premise – Minimum monitoring of systems and networks – Routers have inadequate security mechanisms in place – Potential WIFI connection
001, 002	Employees	**Accidental Threat** Human Error or Failure	– Lax passwords policy – Overworked staff
020, 021, 022, 023, 024, 025, 026, 027, 028, 029, 030	Data	**Deliberate Threat** Information Extortion	– Lax security controls such as encryption techniques. – Disgruntled employee or contractor. – Lax recruiting processes. – External agents have access to the data centre. – Minimum monitoring is done while external agents are present within the premise – Minimum monitoring of systems and networks

			– Routers have inadequate security mechanisms in place
008, 009, 010, 017	Procedures	**Deliberate/ Accidental Threat** Missing, Inadequate or incomplete controls	– Lack of authentication controls such as two/multi-factor authentication. – Lax security controls such as encryption techniques.
003, 007, 008, 009, 010, 013, 015, 016, 017	Procedures	**Accidental Threat** Missing, Inadequate or incomplete organisational policy or planning	– Lax password policy – Lax personal devices policy – Time Period of staff access cards too long (2 years). – No strict time allocation given to external agents' access cards. – Minimum monitoring is done while external agents are present within the premise – All staff members have access to the information in the physically locked external drive. – CCTV recordings get rewritten every 3 days; a short period of time. – Lax security controls such as encryption techniques.
051, 052	Hardware	**Technical Failures** Quality of service deviations between different providers	– Primary and secondary links have different speeds
023, 042, 046, 047	Hardware, Software	**Deliberate Threat** Sabotage or Vandalism	– Web Server in DMZ – Lax virtual security controls. – Lax recruiting processes.
031, 032, 033, 034, 035, 036, 037, 038, 039, 040, 041, 042, 043, 044, 045, 046, 047, 048	Software	**Deliberate Threat** Software Attacks	– Lack of software maintenance – Staff lacking adequate knowledge – Using discontinued or outdated software and packages – Use of opensource, free software – Potential use of personal devices – Only detection/security system is SNORT – Web Server in DMZ

031, 032, 033, 034, 035, 036, 037, 038, 039, 040, 041, 042, 043, 044, 045, 046, 047, 048, 042, 046, 049, 050, 051, 052, 053, 054, 055, 056, 057, 058, 059, 060, 061, 062	Hardware, Software	**Deliberate/ Accidental Threat** Technological Obsolesce	– Lack of scheduled updating and testing of software and hardware
001 ,002	Employees, Hardware	**Deliberate/ Accidental Threat** Fire	- Overworked staff – Disgruntled employee or contractor. – Lax recruiting processes. – External agents have access to the data centre. – Minimum monitoring is done while external agents are present within the premise – Lack of backup generators
020, 021, 022, 023, 024, 025, 026, 027, 028, 029, 030	Data	**Accidental Threat** Data Breach	– Lack of software maintenance – Lax security controls such as encryption techniques.

5.3 Vulnerability Likelihood and Severity

Vulnerability	Likelihood	Severity
Lax physical security controls.	0.6	Significant
Disgruntled employee or contractor.	0.7	Severe
Lax recruiting processes.	0.6	Severe
External agents have access to the data centre.	1.0	Moderate
Minimum monitoring is done while external agents are present within the premise	1.0	Moderate
Lack of security education and training	0.8	Moderate
Minimum monitoring of systems and networks	0.7	Significant

Routers have inadequate security mechanisms in place	0.6	Moderate
Lack of backup generators	0.9	Severe
Potentially faulty equipment	0.5	Moderate
Staff lacking adequate knowledge	0.5	Moderate
Power not distributed adequately	0.4	Significant
Incorrect temperature	0.2	Severe
Lack of failsafe in the event of a fire or natural event.	0.7	Severe
Using discontinued or outdated software and packages	0.6	Moderate
Untested or minimally tested, released software	0.5	Moderate
Datacentre is in the CBD near big buildings and the sea	1.0	Minimal
Suitable controls not provided	0.6	Minor
Lax virtual security controls	0.8	Significant
Routers have inadequate security mechanisms in place	0.6	Significant
Lax passwords policy	0.9	Moderate
Overworked staff	1.0	Significant
Lax security controls such as encryption techniques.	1.0	Significant
Lack of authentication controls such as two/multi-factor authentication.	1.0	Moderate
Lax personal devices policy	0.6	Significant
Time Period of staff access cards too long (2 years).	1.0	Minimal
No strict time allocation given to external agents' access cards.	1.0	Moderate

All staff members have access to the information in the physically locked external drive.	1.0	Moderate
CCTV recordings get rewritten every 3 days; a short period of time.	1.0	Moderate
Primary and secondary links have different speeds	1.0	Minor
Web Server in DMZ	1.0	Moderate
Lack of software maintenance	0.6	Moderate
Use of opensource, free software	1.0	Moderate
Only detection/security system is SNORT	1.0	Severe
Lack of scheduled updating and testing of software and hardware	1.0	Significant

6. Risk Assessment

The analysis of the system's vulnerabilities, the threats associated with them, and the probable impact of that vulnerability exploitation results in a risk rating for each missing or partially implemented control. The risk level is determined on the following two factors:

1. Likelihood of Occurrence
   It is the probability that a specific vulnerability within Data Link will occur.

2. Impact
   It is the consequence of an event, if it occurs.

The risk rating is the point where the likelihood and impact ratings intersect.

Impact						
	Severe	15	19	22	24	25
	Significant	10	14	18	21	23
	Moderate	6	9	13	17	20
	Minor	3	5	8	12	16
	Minimal	1	2	4	7	11
		Almost never	Possible but unlikely	Possible	Highly probable	Certain
		Likelihood				

The consequence of an event may also result in the loss of availability, integrity or confidentiality of information which could lead to:

- Economic loss
- Additional costs being incurred
- Unable to operate
- Staff injury
- Legal liabilities and/or breach of Service Level Agreements
- Disruption of business operations
- Competitive advantage
- Theft of information
- Identity and financial theft
- Loss of corporate or public image

6.1 Security Risks

Risk ID	Threat	Risk Description	Consequence	Impact	Likelihood	Risk Rating
R01	**Deliberate Threat** Theft and fraud	Hardware is stolen from HostNZ.	– Loss of corporate or public image – Disruption of business operations – Economic loss – Unable to operate	Severe	Possible, but unlikely	19
R02	**Deliberate Threat** Theft and fraud	Data is stolen from HostNZ.	– Economic loss – Legal liabilities and/or breach of Service Level Agreements – Disruption of business operations – Theft of information – Identity and financial theft – Loss of corporate or public image	Severe	Possible	22
R03	**Technical Failures** Hardware Failures or Errors	Some servers fail, and customers cannot get access to their paid services	– Unable to operate – Loss of corporate or public image – Disruption of business operations	Moderate	Possible	13
R04	**Technical Failures** Hardware Failures or Errors	Airconditioning stops working	– Economic loss – Additional costs being incurred – Unable to operate – Disruption of business operations	Moderate	Possible, but unlikely	9
R05	**Technical Failures** Software Failures or Errors	Intelligent Air Flow stops working.	– Economic loss – Additional costs being incurred – Unable to operate Disruption of business operations	Moderate	Possible, but unlikely	9
R06	**Technical Failures**	Independent purchasing system fails.	– Economic loss – Disruption of business operations	Moderate	Possible, but unlikely	9

	Software Failures or Errors		– Loss of corporate or public image			
R07	**Natural Disaster** Forces of nature	Tsunami/ Earthquake/ Volcanic occurs.	– Economic loss – Additional costs being incurred – Unable to operate – Staff injury – Disruption of business operations	Severe	Almost never	15
R08	**Deliberate Threat** Espionage or trespass	A competitor's employee is hired and they learn company secrets and get access to private information in the locked external drive.	– Economic loss – Additional costs being incurred – Competitive advantage – Loss of corporate or public image	Moderate	Possible, but unlikely	9
R09	**Deliberate Threat** Espionage or trespass	Malware on routers	– Economic loss – Additional costs being incurred – Legal liabilities and/or breach of Service Level Agreements – Theft of information – Identity and financial theft – Loss of corporate or public image	Severe	Possible	22
R10	**Accidental Threat** Human Error or Failure	Passwords are too easy and staff are victims of a security breach	– Additional costs being incurred – Theft of information – Identity and financial theft – Loss of corporate or public image	Moderate	Possible	13
R11	**Accidental Threat** Human Error or Failure	Staff member falls asleep on the job and work gets backed up	– Economic loss – Disruption of business operations	Minor	Possible	9
R12	**Accidental Threat** Human Error or Failure	Staff member interacts with a phishing email	– Additional costs being incurred – Theft of information	Minor	Highly Probable	12
R13	**Accidental Threat**	Staff member specialising in	– Economic loss – Additional costs being incurred	Severe	Highly Probable	24

	Human Error or Failure	software is rostered on and has to fix a hardware issue that they are not familiar with. They do it wrong and the issue propagates through the data centre (vice versa if specialising in hardware and have to fix software issues)	– Unable to operate – Disruption of business operations – Loss of corporate or public image			
R14	**Deliberate Threat** Information Extortion	Threat actors bypass routers and encrypt information and will not release data until paid.	– Economic loss – Additional costs being incurred – Unable to operate – Disruption of business operations – Theft of information – Identity and financial theft – Loss of corporate or public image	Severe	Possible	22
R15	**Deliberate/ Accidental Threat** Missing, Inadequate or incomplete controls	Email communications are compromised due to a lack of encryption and therefore, user authentication is stolen.	– Economic loss – Additional costs being incurred – Legal liabilities and/or breach of Service Level Agreements – Disruption of business operations – Theft of information – identity and financial theft – Loss of corporate or public image	Severe	Possible	22
R16	**Technical Failures** Quality of service deviations between	When the primary link has an outage and the secondary link is used, services are much slower than usual.	– Competitive advantage	Minimal	Possible	4

	different providers					
R17	**Deliberate Threat** Sabotage or Vandalism	Threat actors get access to the web site and deface it	– Disruption of business operations – Loss of corporate or public image	Minor	Possible	8
R18	**Deliberate Threat** Software Attacks	DDos Attacks occur	– Unable to operate – Loss of corporate or public image	Minor	Possible	8
R19	**Deliberate/ Accidental Threat** Technological Obsolesce	Assets such as smoke alarms; air conditioning units, not reviewed, tested, maintained and updated in a consistent and timely way.	– Additional costs being incurred – Staff injury – Legal liabilities and/or breach of Service Level Agreements – Disruption of business operations	Minor	Possible, but unlikely	5
R20	**Deliberate/ Accidental Threat** Fire	Fire starts near or on premises.	– Economic loss – Additional costs being incurred – Unable to operate – Staff injury – Disruption of business operations	Severe	Possible	22
R21	**Accidental Threat** Data Breach	One customer gains unauthorised access to confidential information of another customer due to failure of controls that provide separation of memory and storage.	– Economic loss – Additional costs being incurred – Legal liabilities and/or breach of Service Level Agreements – Disruption of business operations – Theft of information – Identity and financial theft – Loss of corporate or public image	Severe	Possible	22

6.2 Risk Controls

The following outline methods of mitigating the identified risks. It outlines pre-existing safeguards and ways of improving them. It then provides the new risk rating with the recommended controls. Threat agents are listed in order of their risk rating from the table in the previous section.

Risk ID	Threat Agent	Existing Safeguards	Recommended Controls	Impact	Likelihood	Risk Rating
R13	**Accidental Threat** Human Error or Failure	– Engineers hired with some knowledge of both software and hardware components	– Hire more task-specific engineers and staff	Significant	Possible	18
R02	**Deliberate Threat** Theft and fraud	– Key is given to all staff members. – Safe is used with only the CEO given accessibility rights – The use of SNORT intrusion detection – Access cards used for accountability and potential physical detection of threat actors	– Reduce the number of staff that keys are distributed to – More stringent background checks need to be used during the hiring process – More intrusion detection and prevention systems need to be used. – External staff access cards need to have a time limit, and they need to be more closely monitored when on premises. – Staff access cards should reset less than every 18 months.	Moderate	Possible	13
R09	**Deliberate Threat** Espionage or trespass	– The use of SNORT intrusion detection	– More intrusion detection and prevention systems need to be used. – Engineers need to do routine checks – More stringent background checks need to be used during the hiring process	Minor	Highly Probable	12

R14	**Deliberate Threat** Information Extortion	– The use of SNORT intrusion detection – Engineers advised not to use their own devices for tasks – Strong passwords are expected on devices – Ports are closed	– More intrusion detection and prevention systems need to be used. – Engineers need to do routine checks – Engineers strictly should not use personal devises for work – Strong password policy should be enforced – More stringent background checks need to be used during the hiring process	Minor	Highly Probable	12
R15	**Deliberate/ Accidental Threat** Missing, Inadequate or incomplete controls	– SSH protocol in use – Authenticate with customer details	– Email encryption should be used – Two/Multi-factor authentication should be implemented on login/deletion/cancellation.	Moderate	Possible	13
R20	**Deliberate/ Accidental Threat** Fire	– Protection devices exist (smoke detectors and extinguishers).	– Add more protection devices to the premises – Have backup components – Business Continuity Plan – Human Resources Process – More stringent background checks need to be used during the hiring process – Have a first aid kit on hand	Significant	Possible	18
R21	**Accidental Threat** Data Breach	– Linux in-built memory protection	– Add more memory protection – Less use of local storage	Minor	Possible	8
R01	**Deliberate Threat** Theft and fraud	– Key is given to all staff members. – Safe is used with only the CEO given accessibility rights – Access cards used for accountability and potential physical	– Reduce the number of staff that keys are distributed to – More stringent background checks need to be used during the hiring process – External staff access cards need to have a time limit, and they need to be more	Moderate	Possible, but unlikely	9

		detection of threat actors	closely monitored when on premises. – Staff access cards should reset less than every 18 months.			
R07	**Natural Disaster** Forces of nature	– Protection devices exist (smoke detectors and extinguishers).	– Move out of the CBD into a more rural in Auckland – Add backup components – Business Continuity Plan – Human Resources Process – Add more protection devices to the premises – Have a first aid kit on hand	Significant	Almost never	10
R03	**Technical Failures** Hardware Failures or Errors	– Use of multiple servers – Air conditioning in use – Power Distribution module in use	– Add backup components – Business Continuity Plan – Use more servers	Minor	Possible	8
R10	**Accidental Threat** Human Error or Failure	– Engineers are expected to use strong passwords for devices.	– Enforce a stronger password policy	Minor	Possible	8
R12	**Accidental Threat** Human Error or Failure		– Include security training as an ongoing training process that all staff members must participate in	Minimal	Possible, but unlikely	2
R04	**Technical Failures** Hardware Failures or Errors		– Add backup components – Business Continuity Plan	Minimal	Possible, but unlikely	2
R05	**Technical Failures** Software Failures or Errors		– Add backup components – Business Continuity Plan	Minimal	Possible, but unlikely	2
R06	**Technical Failures** Software Failures or Errors		– Have more than one web/application server – Provide an alternative purchasing system	Moderate	Possible, but unlikely	9

R08	**Deliberate Threat** Espionage or trespass		– Reduce the number of staff that keys are distributed to – More stringent background checks need to be used during the hiring process – External staff access cards need to have a time limit, and they need to be more closely monitored when on premises. – Staff access cards should reset less than every 18 months.	Moderate	Almost Never	6
R11	**Accidental Threat** Human Error or Failure	– Rotational shifts	– Hire more engineers	Minor	Almost Never	3
R17	**Deliberate Threat** Sabotage or Vandalism	– Use of a bastion host – Only staff have immediate access to it	– More stringent background checks need to be used during the hiring process – Business Continuity Plan – Human Resources Process – Remove server from DMZ	Minor	Possible, but unlikely	5
R18	**Deliberate Threat** Software Attacks	– The use of SNORT intrusion detection – Ports are closed	– Business Continuity Plan – Secure Network infrastructure – Develop a DDos Response Plan	Minor	Possible	8
R19	**Deliberate/ Accidental Threat** Technological Obsolesce		– Include more testing – More asset monitoring – More maintenance	Minor	Possible, but unlikely	5
R16	**Technical Failures** Quality of service deviations between different providers	– Primary link predominantly used, secondary only in use in case of an outage	– Ensure secondary option has same or similar speed → ~10gbps	Minimal	Possible, but unlikely	2

7. Bibliography

[1] Department of Internal Affairs, “Risk Assessment Process — Information Security,” digital.govt.nz, February 2014. [Online]. Available: https://www.digital.govt.nz/dmsdocument/3-risk-assessment-process-information-security/html#1-introduction. [Accessed 10 August 2020].

[2] M. Rouse, “software license,” techtarget, [Online]. Available: https://searchcio.techtarget.com/definition/software-license. [Accessed 16 August 2020].

[3] Apache OpenOffice, “Why Apache OpenOffice,” Apache, [Online]. Available: https://www.openoffice.org/why/index.html. [Accessed 16 August 2020].

[4] Snort, “Snort,” https://www.snort.org/, [Online]. Available: https://www.snort.org/. [Accessed 16 August 2020].

[5] N. Malaval, “How to Record SSH Sessions Established Through a Bastion Host,” AWS, 14 June 2016. [Online]. Available: https://aws.amazon.com/blogs/security/tag/bastion-host/. [Accessed 16 August 2020].