Assignment One

1. Overview

TrueServer is a small sized data centre which provides virtual, shared and dedicated Private Servers (VPS) to consumers in New Zealand. The data centre is located at Wellington Central Business District (CBD) on floor 1 of 12 Customhouse Quay Street. The company relocated to the new data centre 2 years ago. Businesses located in Wellington contribute to a large portion of TrueServer's customers at the moment.

2. Classification definitions

CIA Triad

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

Asset 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 internal company information that can be viewed by employees, as well as authorised third parties. Not necessarily sensitive data, so requires less protection than confidential assets.
Public/External	Used for information that has been approved for public release. Requires less protection than confidential or internal assets.

Likelihood

Likelihood	Description
Certain	It would be easy for a threat to exploit the vulnerability without any specialised skills or resources.
Highly probable	It is feasible for a threat to exploit the vulnerability without any specialised skills or resources.
Possible	It is feasible for a threat to exploit the vulnerability, given moderate specialised skills or resources.
Possible but unlikely	It is feasible for a threat to exploit the vulnerability, but would require significant skills or resources to do so.

Almost never	It would be difficult for a threat to exploit the vulnerability regardless of skills or resources.

Impact/Severity

Impact	Description
Severe	There is economic loss. There is loss of life. Legal liabilities and/or breach of SLAs. There is loss of corporate or public image. Communications and recovery must be shared with customers. Impact cannot be managed without significant extra costs. Ongoing impact on service delivery.
Significant	There is economic loss. There is serious physical harm. Some legal liabilities and/or breach of SLAs. There is loss of corporate or public image. Communications and recovery are shared with customers. Impact cannot be managed without extra costs. Ongoing impact on service delivery.
Moderate	There is limited economic loss. There is minor physical harm. Limited legal liabilities and/or breach of SLAs. Limited loss of corporate or public image. Communications and recovery may be shared with customers. Limited impact on service delivery. Impact can be managed with limited extra costs.
Minor	There is minor economic loss. There is no physical harm. Minor legal liabilities and/or breach of SLAs. Minor loss of corporate or public image. Communications and recovery do not need to be shared with customers. Internal communication may be necessary. Minor impact on service delivery. Impact can be managed without extra costs.
Minimal	No economic loss. No physical harm. No legal liabilities and/or breach of SLAs. No communications internally needed. No impact on service delivery. Impact can be managed business as usual.

Valuation Criteria

Impact	Description
High	It will result in a loss of concern between TrueServer and its customers or result in a large legal action or cause TrueServer significant revenue or earnings loss.
Medium	It will result in potential legal action or cause some loss of reputation for TrueServer or cause revenue or earnings loss.
Low	It will result in potential minor revenue loss or minor loss of reputation with customers of TrueServer.

Asset Categories

Asset Category	Description
Employees	Any member of staff at TrueServer.
Procedures	IT actions and standard methods of completing tasks and operations.
Software	Applications, operating systems and security components used by TrueServer.
Hardware	Physical equipment used by TrueServer in providing their services.
Data	Information both on users and their transactions, as well as on TrueServer company activities.
Infrastructure	Supplementary equipment required to keep the datacentre safe and operational.

3. Roles and Responsibilities

Role	Description and Responsibilities
Chief Executive Officer (CEO)	The CEO owns and manages the company and is responsible for coordinating day-to-day activities. Other duties include: - Issue RFID access - Managing financial data - Hiring and termination of employees
Engineer	There are 2 engineers who provide 24/7 support to customers through 12-hours shifts. Engineers have full access to the user account information. Some of their other duties include: - Register new users - Activate or deactivate user accounts - Delete use accounts and data - Backup - System maintenance and upgrades - Password reset Engineers are also responsible for ensuring all hardware components work properly, manage electrical systems within the data centre, wiring, cooling systems etc.

4. Information assets and classifications

People Assets

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

Procedure Assets

Item ID	Asset Category	Asset Name	Asset Description/Attribute	
003	Procedures	Personal Use of Devices Policy	Policy: Purpose:	Engineers are advised to avoid using their personal devices such as laptops or tablets to perform daily tasks. They are provided with desktop PCs instead. Protect TrueServer assets against any malicious software that may infect engineers' personal devices; maintain confidentiality and integrity of TrueServer data.
004	Procedures	Customer Purchase Policy	Policy: Purpose:	All purchases of TrueServer services must be conducted through the online purchase system. Payments are done using an external system such as PayPal. No credit card information is shared with TrueServer. To protect the integrity of transactions and ensure that services are not activated without payment and validation to prevent loss of income. Protects customer credit card information in the event of a data breach which could potentially open TrueServer up to liability.
005	Procedures	Transaction Data Storage Policy	Policy: Purpose:	Transactional data including customer number, customer email, full name and address is to be stored on a NAS drive located in the office supply room in .csv format. To ensure the confidentiality and integrity of TrueServer customer information; minimise risk of customer information lost in a data breach.
006	Procedures	Customer Login Policy	Policy: Purpose:	Customers log into their VPS system through SSH service. Each customer has their own system which is separate from others, overall protecting the confidentiality, integrity and availability of assets.
007	Procedures	VPS Reset Policy	Policy: Purpose:	Customers can reset their VPS through logging into a management interface. Credentials are emailed to their registration email. VPS management system passwords can be reset by phone or email. To ensure that customers have the ability to reset their VPS but cannot reset their VPS by accident in order to protect integrity and availability of customer data.
008	Procedures	Cancellation of Service Policy	Policy: Purpose:	Customers can use the management interface to cancel their service immediately. They will be presented with a confirmation link. If confirmed, their service will be cancelled and the account and data are immediately deleted. To ensure that customers are able to cancel their service when desired without

				difficulty. Protects confidentiality of the data on their VPS, as well as their customer data.
009	Procedures	Employment Document Storage Policy	Policy: Purpose:	Employment documents are kept in a safe in the CEO's office. Only the CEO has access to this safe. To maintain confidentiality and integrity of employment information, and to protect TrueServer employee data against threat actors.
010	Procedures	Physical Access Policy	Policy: Purpose:	Physical access to the datacentre is approved by the CEO via RFID cards. Engineers are issued cards granting access to their own office, the supply room and the server room. All RFID access is logged to the CEO's PC. To prevent unauthorised access to TrueServer assets and ensure that any employee misuse can be tracked by the CEO.
011	Procedures	Employee Password Policy	Policy: Purpose:	Engineers are expected to use strong passwords for devices. Protect TrueServer assets from unauthorised access, maintain confidentiality and integrity of data.
012	Procedure	Wireless Access Policy	Policy: Purpose:	Employees are not provided with wireless access at work. Prevent exposure of TrueServer assets to malicious software or viruses, maintaining confidentiality and integrity of TrueServer data.
013	Procedure	External Contractor Policy	Policy: Purpose:	All office maintenance is conducted by external contractors. They are provided with temporary access when required. Protect TrueServer assets against threat actors, maintain confidentiality and integrity of data.
014	Procedure	Customer Data Monitoring Policy	Policy: Purpose:	TrueServer does not monitor customer data or software on their VPS. Protect TrueServer from legal liability in the event of a customer using their VPS for illegal purposes.
015	Procedure	Customer Port Access Policy	Policy: Purpose:	All ports to and from the DMZ are open for customers. This allows them to connect from any port or service and to connect to external resources from their VPS server. Ensure availability of data for TrueServer clients.
016	Procedure	Internal Subnet Policy	Policy: Purpose:	All TrueServer internal devices such as engineers' Desktop PCs and the NAS drive are located within an internal subnet isolated by a firewall. Protect TrueServer assets against threat actors, maintain confidentiality and integrity of data.

Data Assets

Item ID	Asset Category	Asset Name	Asset Description/Attribute	Classification
017	Data	Customer Account Information	Detailed information on customers and transactions, including home address, email and phone number. Owner: TrueServer	Confidential.
018	Data	Employment Data	Information on TrueServer employee contracts, terms of employment, etc. Owner: TrueServer	Confidential
019	Data	User Login Details	Information used to log in to VPS services; username, password, VPS IP address. Owner: TrueServer/Customer	Private
020	Data	Service Information	Information displayed on TrueServer's website with regards to a service – Basic, Advanced, Premium and relevant info to each. Owner: TrueServer	Public
021	Data	Customer Data	Data kept on VPS systems by customers. Owner: Customer	Private
022	Data	VPS System Information	Information on the specifics of a purchased VPS system. Owner: TrueServer/Customer	Private

Software Assets

Item ID	Asset Category	Asset Name	Asset Description/Attribute
023	Software	Firewall	Network security system that controls incoming and outgoing network traffic based on a set of rules.
024	Software	Email	Email service used to communicate with customers.
025	Software	Debian 6.0 Linux Distribution	Linux distribution which the hypervisor runs on.
026	Software	Ubuntu Desktop Distributions	Default operating system for all TrueServer desktop PCs.
027	Software	OpenOffice	Free and open-source office suite for word processing, spreadsheets, presentations etc.
028	Software	Hypervisor	Creates and runs virtual machines
029	Software	VPS Management System	Manages the Virtual Private Servers rented by customers.

030	Software	SSH Service	A network protocol for operating network services securely. Used for customer access to their VPS.
031	Software	Web Server	Server which hosts the TrueServer website.
032	Software	Server	Dedicated servers which host the virtual servers.
033	Software	Virtual Server	The virtual servers that customers pay for access to.
034	Software	RFID Access Software	GAO RFID Access Control Software which allows for ID card reading and calibration of access to areas of the datacentre.
035	Software	NAS Backup Software	Software for the Network Attached Storage drive used to back up transactional data and customer information.

Hardware Assets

Item ID	Asset Category	Asset Name	Asset Description/Attribute
036	Hardware	Server	Description: High density heat and dedicated servers. Quantity: 24 Category: Systems and peripherals Location: Server Room
037	Hardware	Web Server	Description: Dedicated server for website hosting. Quantity: 1 Category: Systems and peripherals Location: Server Room
038	Hardware	Port Switches	Description: Connects devices on a network Quantity: 24 Category: Network components and equipment Location: TrueServer office
039	Hardware	Routers	Description: Forward data packets to different parts of a network Quantity: 3 Category: Network components and equipment Location: TrueServer office
040	Hardware	Data Link	Description: Provides 10gbps primary link to a network provider Quantity: - Category: Network components and equipment Location: TrueServer office
041	Hardware	Desktop PCs	Description: Dedicated PCs used by all staff Quantity: 3 Category: Systems and peripherals Location: TrueServer office
042	Hardware	Access Cards	Description: Cards used for access to TrueServer premises. Quantity: 3 Category: Security devices Location: TrueServer office
043	Hardware	NAS Drive	Description: Network Access Storage Drive Quantity: 1 Category: Systems and peripherals

			Location:	Supply room
044	Hardware	Safe	Description: Quantity: Category: Location:	Safe for storage of employment documents. 1 Security devices CEO's Office

Infrastructure Assets

Item ID	Asset Category	Asset Name	Asset Description/Attribute	
045	Infrastructure	Smoke Detectors	Description: Quantity: Category: Location:	Smoke detectors to alert if there is a fire. 4 Protection devices TrueServer office
046	Infrastructure	Air Conditioning System	Description: Quantity: Category: Location:	Controls temperature in the building. 1 Protection device TrueServer office
047	Infrastructure	Power Distribution Module	Description: Quantity: Category: Location:	Distributes electricity to the various data servers. 2 Protection device Server room
048	Infrastructure	Access Card System	Description: Quantity: Category: Location:	Allows access to different areas of the building. 6 (one per door) Protection device, detection device Server room door, all office doors, main door, supply room door

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 Purchase Policy	Low	Low	Low
005	Transaction Data Storage Policy	High	Low	Medium
006	Customer Login Policy	Low	Low	Low
007	VPS Reset Policy	Low	Low	Low

008	Cancellation of Service Policy	Low	Low	Medium
009	Employment Document Storage Policy	High	Low	Low
010	Physical Access Policy	Medium	Medium	Low
011	Employee Password Policy	High	High	High
012	Wireless Access Policy	Medium	Medium	Medium
013	External Contractor Policy	Medium	Medium	Medium
014	Customer Data Monitoring Policy	Low	Low	Medium
015	Customer Port Access Policy	Low	Low	Medium
016	Internal Subnet Policy	Medium	Medium	Medium
017	Customer Account Information	Medium	Low	Low
018	Employment Data	High	High	Low
019	User Login Details	High	High	High
020	Service Information	Low	High	High
021	Customer Data	Medium	Medium	Medium
022	VPS System Information	Medim	Medium	Medium
023	Firewall	High	High	High
024	Email	High	High	High
025	Debian 6.0 Linux Distribution	Medium	Medium	Medium
026	Ubuntu Desktop Distributions	Low	High	Medium
027	OpenOffice	Low	Low	Medium
028	Hypervisor	Low	Medium	High
029	VPS Management System	Medium	High	High
030	SSH Service	Medium	High	High
031	Web Server Software	Medium	High	High

032	Server Software	High	High	High
033	Virtual Server	High	High	High
034	RFID Access Software	High	High	High
035	NAS Backup Software	High	High	High
036	Server	High	High	High
037	Web Server	Medium	High	High
038	Port Switches	High	High	Medium
039	Routers	High	High	High
040	Data Link	High	High	High
041	Desktop PCs	Medium	High	Medium
042	Access Cards	High	High	High
043	NAS Drive	High	High	Medium
044	Safe	High	High	High
045	Smoke Detectors	Medium	High	High
046	Air Conditioning System	Low	Medium	Medium
047	Power Distribution Module	Medium	High	High
048	Access Card System	High	High	High
049	Intelligent Airflow System	Low	High	High

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 TrueServer 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				

Security Risks

Risk ID	Asset ID(s)	Threat	Vulnerability	Risk Description	Consequence	Gross Risk		
						Impact	Likelihood	Risk Rating
R01	036, 037, 039, 041, 042, 043, 017, 018	Theft	– There is no screening, monitoring or logging process for employees entering the company premise.	- This allows a disgruntled employee to steal the asset.	Economic loss Disruption of business operations Potential legal liabilities Depending on assets stolen, potentially unable to operate Theft of information	Severe	Highly Probable	24
				- This allows an outsider to enter the premise and steal the asset.	Economic loss Loss of confidentiality Disruption of business operations Potential legal liabilities Depending on assets stolen, potentially unable to operate Theft of information	Severe	Possible but unlikely	19
R02	001, 002	Human Error	– Overworked staff – Lack of background checks	- Staff member falls for phishing email	Theft of information Potential additional costs	Moderate	Possible	13
				- Staff member falls asleep on the job	Economic loss Disruption of business operations	Minor	Possible	9
				- Staff member is required to do a job they lack the knowledge to do. They do it wrong, leading to issues through the datacentre.	Economic loss Disruption of business operations Loss of corporate or public image Additional costs incurred to fix issues.	Significant	Possible	18
				- Passwords are too easy and staff are victims of a security breach	Additional costs incurred Theft of information Identity or financial theft Loss of corporate or public image	Moderate	Possible	13
R03	001, 002, 036, 037, 038, 039,	Fire	– Lack of adequate fire detection and suppression system	- A fire could potentially start and reach all sections of the building	Staff injury or loss of life Legal liabilities as a result of loss of life Unable to operate Economic loss Additional costs for repairs to premises	Severe	Possible	22

	041, 042, 043, 017, 018, 044, 045, 046, 047, 048, 019, 020, 021, 022							
R04	017, 018, 019, 020, 021, 022, 023, 031, 032, 028, 027, 033, 035	Espionage or trespass	– Lax physical security controls – Lax virtual security controls – Disgruntled employee or contractor – External agents have unmonitored access to the datacentre	- A competitor's employee is hired and is able to access confidential data.	Economic loss Loss of competitive advantage Loss of corporate or public image Potential additional costs	Significant	Possible but unlikely	14
				- The firewall is breached and the internal routers are exposed to malware	Economic loss Potential additional costs Theft of information Legal liabilities and/or breach of SLAs Identity theft Loss of corporate or public image	Severe	Possible	22
R05	023, 031	Sabotage or vandalism	– Lax recruiting procedures – Web server in DMZ – Lax virtual security controls	- Threat actors gain access to the website and deface it	Disruption of business operations Loss of corporate or public image	Minor	Possible	8
R06	040, 046, 049	Technical Failures	– Lack of backup data link – Lack of backup power generation – Lack of backups for important systems	- The data link fails, rendering services unavailable to customers	Disruption of business operations Loss of corporate or public image Loss of competitive advantage Additional cost of repair	Minor	Possible	8
				- Air conditioning or intelligent airflow stops working	Economic loss Additional costs incurred Unable to operate Disruption of business operations	Moderate	Possible but unlikely	9

				- Power outage on the premises	Unable to operate Economic loss Disruption of business operations	Moderate	Possible	13
R07	024, 028, 029, 030, 031, 032	Software Attacks	– Web server in DMZ – Lax recruiting procedures – Using discontinued or outdated software	- DDoS attacks occur	Unable to operate Loss of corporate or public image	Minor	Possible	8
R08	045, 046, 047, 049, 034	Technological obsolescence	– Lack of scheduled updating and testing of hardware/software	- Assets such as smoke alarms, A/C units not reviewed, tested and maintained in a consistent manner	Additional costs incurred Economic cost Unable to operate Potential staff injuries Potential legal liability for said injuries Disruption of business operations	Significant	Possible but unlikely	14
R09	019, 021, 022, 029, 030, 033	Data Breach	– Lack of software maintenance – Lax security controls in areas such as encryption	- One customer gains unauthorised access to confidential information of another customer due to a failure in controls that provide separation of memory and storage.	Economic loss Legal liabilities/breach of SLAs Disruption of business operations Theft of information Identity and financial theft Loss of corporate or public image	Severe	Possible	22
R10	001, 002, 036, 037, 038, 039, 041, 042, 043, 017, 018, 044, 045, 046, 047, 048, 019, 020, 021, 022	Natural disaster	– Lack of backup generators – Suitable controls not provided	- A tsunami or earthquake occurs in the Wellington region that damages the datacentre.	Staff injury or loss of life Legal liabilities as a result of loss of life Unable to operate Economic loss Additional costs for repairs to premises	Severe	Possible but unlikely	19

R11	017, 018, 019, 020, 021, 022	Information Extortion	– Lax recruiting process – Disgruntled employee – Minimum monitoring of systems and networks – External agents allowed unmonitored in datacentre – Lax security controls such as encryption techniques	- Threat actors bypass routers and encrypt information, will not release unless paid	Economic loss Additional costs incurred Unable to operate Disruption of operations Identity and financial theft Theft of information Loss of corporate or public image	Severe	Possible	22
R12	021, 024, 029, 030	Email compromised	– Lack of authentication controls such as 2FA – Lax security controls such as encryption techniques	- Email communications are compromised due to a lack of encryption and therefore user information is stolen	Economic loss Legal liabilities/breaches of SLA Disruption of operations Theft of information Identity theft Loss of corporate or public image	Severe	Possible	22
R13	042, 048	Access stolen	– Access cards kept by employees – Lack of protocol to disallow access outside of work hours	- A threat actor steals an employee's ID card.and uses it to enter the premises.	Economic loss Disruption of operations Theft of information Financial theft	Significant	Possible	18
R14	017, 035, 043	Backup failure	– Lack of off-site backup – Backup only once per week	- The NAS backup software fails or is unable to run properly, leading to customer information not being saved correctly	Disruption of operations Loss of corporate or public image	Minor	Possible but unlikely	5
				- The NAS drive is lost, damaged or destroyed	Disruption of operations Loss of corporate or public image Economic loss Potentially unable to operate altogether	Significant	Possible but unlikely	14
R15	018, 044	Loss of safe key	– Only one safe key in possession of CEO	- The CEO loses the key to the safe, rendering the employment documents	Disruption of operations Additional costs for key replacement	Moderate	Possible	13

				inaccessible.				

Risk Controls

The following table outlines methods for mitigating the identified risks. It identifies existing safeguards and recommends methods for improving them to reduce the probability of a given risk and mitigate in the event it does happen.

Recommended Controls

Risk ID	Existing safeguards	Recommended Controls
R01	• Access cards are required to enter the premises.	• Install CCTV cameras in the office, supply room and server room. • Require all employees and visitors to sign in before entering the premises.
R02	• Engineers hired with some knowledge of hardware and software elements of the work.	• Implement stronger background checks in the recruiting process to verify employee credentials. • Hire additional staff to reduce individual workload and increase productivity. • Run semi-regular phishing tests on employees to ensure they can recognise an attempt.
R03	• smoke detectors currently installed. • Backup available.	• Business Continuity Plan including a cold site • Additional standard-compliant smoke detectors must be installed • Back up of essential company data must be kept off premise (e.g. on the cloud) • Install fire extinguishers on TrueServer premises
R04	• Access cards required to enter the premises • Contractor access is temporary and issued by the CEO • Firewall installed and office not given wireless access.	• More stringent background checks in the recruiting process. • Install an intrusion detection/prevention system. • Require contractors to be monitored during their work.

R05	• Only staff have immediate access to the web server.	• Add a bastion host to the network. • Remove web server from DMZ.
R06	• No existing safeguards	• Install a backup data link to be used in the event of a failure in the primary data link. • Install a backup power generator on the premises to keep systems running in the event of a failure.
R07	• No existing safeguards	• Remove web server from DMZ • Install intrusion detection/prevention software. • Develop a DDoS response plan.
R08	• No existing safeguards	• Require regular testing of important software, hardware and infrastructure assets. • Implement routinely scheduled maintenance of assets.
R09	• Linux built-in memory protection.	• Add more memory protection. • Implement routinely scheduled maintenance and testing of software.
R10	• No existing safeguards	• Move out of Customhouse Quay, as it is a high-risk zone for earthquake and tsunami activity. • Keep first-aid supplies on the premises. • Add more protection devices to the premises.
R11	• Engineers advised not to use their own devices for work. • Strong password policy. • Office does not have wireless access.	• Install an intrusion detection/prevention system. • Mandate routine checks of software • Strong password policy should be more strictly enforced.

R12	• SSH protocol in use • Authenticate with customer details	• Mandate email encryption • Multi-factor authentication should be implemented on login/deletion/cancellation of service.
R13	• CEO can monitor use of access cards • GAO RFID allows for remote shutdown of access cards • 24/7 operation – always someone on-site	• Disallow card access outside of an employee's shift hours • Impose time limits on ID cards – employees must get them replaced regularly.
R14	• NAS drive kept in secure location.	• Increase backup regularity – daily rather than weekly. • Have off-site backup of customer data.
R15	• Key is kept on CEO's person.	• Create spare safe key to be kept by CEO. • Change to combination rather than key-based safe.

Reference List

Whitman, M.E., Mattord, H.J. (2014). *Principles of Information Security* (5th ed.). United States of America: Cengage Learning

Software for RFID access control systems: RFID tracking by Gao. GAO RFID. (2021, March 31). https://gaorfid.com/access-control-software-overview/

Why Apache OpenOffice. Apache OpenOffice. (n.d.). https://www.openoffice.org/why/