CYBR373

Assignment 1

Olivia Fletcher
300534281
fletcholiv

Case Study - QuantumNZ

Introduction

QuantumNZ is a data center based in Wellington, New Zealand which provides a wide variety of services to the public based on a subscription. A large portion of offices within Wellington CBD employ the services offered by Quantum. Such services include; virtual, shared and dedicated private services (VPS). There are many background tasks and processors within Quantum to ensure customer satisfaction, today, we will be assessing inner company processors ranging from employee procedures to server software/hardware to assess the potential security risks that could take place.

Task a

Rating and classification definitions

- Confidentiality, integrity and availability, also known as the CIA triad is a model designed to help specify information security policies for organizations.

CIA Triad	Requirements
Confidentiality	Ensuring that information/data is only accessible to those who are verified or have authorized access.
Integrity	Detections of alterations that occur within data transfers as a means of safeguarding the accuracy of information within company processors.
Availability	Ensuring that authorized users have access to information/data and assets when required.

- Classification

Value	Description
Restricted	Restricted data has the highest of strict security controls to limit access by only allowing access to verified identities. This data bracket tends to be highly monitored to ensure a breach has not taken place. If a data breach were to happen on this level this could potentially destroy a company and its processes.
Confidential	Requires specific authorization or clearance to access data. Tightly secured and monitored to ensure no malicious access.
Private	Data cannot be disclosed to the public but does not require tight security. This bracket of data can be accessed by employed individuals to the company and any verified third-party access. Data breach is possible and a risk but does not contain data which could damage the company.
Public	Does not require much protection and is freely accessible to the public. This data can be freely used, reused and redistributed without damage to the company or individual. This can include but is not limited to; names, job descriptions etc

- Likelihood

LikeliHood	Description
Certain	The vulnerability is exposed and exploitable to those with malicious intent. This exploit could result in severe impacts to the company. Relevant security control is not effective or able to identify how to remediate the exploit.
Highly probable	The vulnerability is of high concern and is on display to those with the knowledge to be able to exploit it. Relevant security control has been planned but not implemented and requires attention making it minimally effective.
Possible	The vulnerability is of moderate concern based on being somewhat exposed for exploitation to those who are looking for it. Relevant security control is planned and partially implemented and is somewhat effective to a potential attack.
Possible but unlikely	The vulnerability is of minor concern but the relevant security in place could be improved upon to avoid further concern. The current remediation security is somewhat effective.
Almost never	The vulnerability is not of a concern to the company cyber resources. The relevant security is effective and fully implemented up to date.

- Impact

Impact	Description
Severe	The incident affects **all** cyber resources which have the ability to significantly damage the company's finances and image. The breach could affect the following company resources; information systems, inner business processors and finances, infrastructure, public/private services and organization structure.
Significant	The incident caused **extensive** damage involving **most** of the cyber resources such as; information systems, inner business processors and finances, infrastructure, public/private services and organization structure.
Moderate	The effects of the incident are **wide-ranging** and affect a **significant-portion** of the cyber resources available to the company.
Minor	The effects of the incident are **minor** involving **some** of the cyber resources.
Minimal	The effects of the incident are **limited** involving **minimal** cyber resources.

- Valuation Criteria

Impact	Description
High	Resulting in high levels of trust lost between Quantum NZ and its customer base. High impact on the financial department and legal actions have taken place against the company.
Medium	Potentially serious adverse effects on organizational operations as the company's financial lessons due to customer decline.
Low	Limited adverse effects on company operations. Customer base lessons but does not directly affect company financials.

Task b

[10] Asset Identification and classification (i.e information asset classification worksheet)

- People's Assets. Employees and contractors

Asset ID	Category	Asset Name	Description and Duties
P01	Staff	CEO	Description includes; - Owns and manages the company. Is responsible for coordinating day-to-day staff activities. Duties include; - Issuing RFID access - Managing financial data - Hiring new employees - Termination of employments
P02	Staff	Engineers	Description includes; - Two individual engineers who are available to provide 24/7 support to customers through interchangeable 12 hour shifts. The engineers have full access to the user account information. Responsible for ensuring all hardware components are functional and managing the data centers wiring and cooling electrical systems. Duties include; - Registering new users - Activate/deactivate user accounts - Delete user accounts and data - Backup system/staff/user data - System maintenance and upgrades - Password resets
P03	Hired Maintenance	Maintenance	Description includes; - Plumbing and cleaning duties are managed by hired external contractors, when hired, workers receive temporary room access depending on duties required. Duties include (but not limited to); - Plumbing - Cleaning

- Hardware Assets. Systems and peripherals, security devices, data centers and networking components.

Asset ID	Category	Asset Name	Description and Attributes

H01	Hardware	Servers	Description;
			- Each server can support up to 20 virtual servers. Servers managed by the engineers.
			Quantity;
			- 24 dedicated servers
			Price (per unit);
			- $15,000, $360,000 all up

H02	Hardware	Web Server	Description includes;
			- Dedicated web server.
			Quantity;
			- 1 WebM server
			Price (per unit);
			- N/A

H03	Hardware	24-Port Switches	Description includes;
			- Hardware component dedicated to handling server switching.
			Quantity;
			- 11
			Price (per unit);
			- $3,000, $33,000 all up

H04	Hardware	Routers	Description includes;
			- Receives and sends data through the network, the routers help improve internet speed and access.
			Quantity;
			- 3
			Price (per unit);
			- $5,000, $15,000 all up

H05	Hardware	Data Link	Description includes;
			- Responsible for multiplexing data streams, data frame detection, medium access and error control.
			Size;
			- 10Gbps
			Price (per unit);
			- N/A

H06	Hardware	Aircon System	Description includes; - Used to cool the temperature within the

			office and server room. Quantity; - 1 Price (per unit); - $2,500

H07	Hardware	Safe	Description includes;
			- CEO keeps employment documents in a safe in his office, CEO is the only staff member with access.
			Quantity;
			- 1

H08	Hardware	Smoke Detectors	Description includes;
			- Off the shelf battery powered smoke detectors, two located in the main office and two located in the server room.
			Quantity;
			- 4
			Price (per unit);
			- $15

H09	Hardware	Power Distribution Module	Description includes;
			- Used to provide electrical power from a main power source and distribute to each equipment within the server and offices.
			Quantity;
			- 2
			Price (per unit);
			- $6,000

H10	Hardware	Network Attached Storage (NAS) Drive	Description includes;
			- Customer transactional information and full account details are saved every Friday on the NAS drive in the office supply room.
			Quantity;
			- 1

H11	Hardware	Staff RFID key	Description includes;
			- Every employee has an RFID key which grants access to their own office, the office supply room and the server room.
			Quantity;
			- 1

- Software Assets. Applications, operating systems and security components.

Asset ID	Category	Asset Name	Description and Attributes

S01	Software	Firewall	Description;
			- All internal devices such as desktop PCs are located within an internal subnet, isolated by the firewall.
			Price;
			- Free

S02	Software	Hypervisor	Description;
			- Hypervisor, a type of a Virtual Machine Monitor (VMM) is a software that creates and runs virtual machines. The servers are managed by Hypervisor which runs on a debian 6 Linux distribution.
			Price;
			- $10,000

S03	Software	Debian 6.0	Description;
			- Debian is a Linux based operating system configured for a range of devices such as laptops, desktops and servers.
			Price;
			- Free

S04	Software	Customer Management Software	Description;
			- CMS is a software tool that is designed to help provide customers with a unique and seamless experience. This provides the customer with their own transactional information and the ability to edit their stored information.
			Price;
			- In-house

S05	Software	Open Office	Description;
			- Open office is an open-source office suite which is used to create documents, presentations, spreadsheets, graphics and databases.
			Price;
			- Free

S06	Software	RFID Access Software	Description; - RFID access is managed and tracked via a unique identifier assigned to each key.

- Data Assets. Information transmissions, processing and storage, databases, hardcopies and intellectual property.

Asset ID	Category	Asset Name	Description and Attributes
D01	Data	Logged Customer Data	Description; - A spreadsheet of customer transactional and personal information is stored in a [.cvs] file in a drive located in the office supply room.
D02	Data	Logged RFID Access Data	Description; - The logged RFID access software data is sent to and saved on the CEOs desktop.
D03	Data	Customer Data	Description; - Customer data represents information the customer keeps on their virtual machine.
D04	Data	Employee Data	Description; - Employee data, personal details, RFID logs and hours/payments.
D05	Data	Financial data	Description; - The CEO manages employee payments and company expenditures.
D06	Data	Backup data	Description; - Engineers responsible for ensuring the servers are sufficiently backed up incase of server drops or technical difficulties.

Weighted Scoring Factor Analysis

Levels	Impact on revenue/profitability/public image Score	Total Score (average between each of the categorizations)
High	0.6-1.0	66-100
Medium	0.3-0.6	33-66
Low	0.0-0.3	0-33

- An example of a **high risk** asset score would be; if the servers were inoperable it would highly disrupt company revenue and profitability as the business operations are fully reliant on the workings of the servers.
- An example of a **medium risk** asset score would be; if the routers were to fail it would disrupt some company processes but overall would not cause the business to shut down.
- An example of a **low risk** asset score would be; If a staff RFID card were to stop working it would be an easy fix for the company and would not disrupt any other business operations.

I believe data assets and some hardware assets will have a heavier high asset risk score rating as the companies data is vital for survival as stored customer data is sensitive and ensured to be private, if a data leak or backup data failure occurs it would devastate the companies public image. Some hardware assets such as the servers themselves are at a high score rating as the company requires working servers to be sufficient in all duties, some hardware elements such as routers or switches are important for server fluidity as it ensures secure connections and networking speeds but is not vital for server operations.

- Information Asset Prioritization Scoring

Asset ID	Classification	Impact on Revenue	Impact on Profitability	Impact on Public Image	Total Score
H01	Confidential	1.0	1.0	0.8	93
H02	Confidential	0.8	0.8	0.5	70
H03	Confidential	0.5	0.7	0.3	50
H04	Confidential	0.5	0.7	0.4	53
H05	Confidential	0.5	0.7	0.3	50
H06	Private	1.0	1.0	0.0	66
H07	Restricted	0.8	0.8	0.0	53
H08	Private	0.8	0.8	0.0	53
H09	Confidential	0.9	0.5	0.3	56
H10	Confidential	1.0	1.0	1.0	100
H11	Confidential	0.3	0.5	0.0	27
S01	Restricted	0.7	0.7	0.0	47
S02	Confidential	0.7	0.5	0.3	50
S03	Confidential	0.3	0.3	0.0	20
S04	Public	0.8	0.8	1.0	87
S05	Public	0.2	0.2	0.0	13
S06	Confidential	0.2	0.2	0.2	20
D01	Restricted	0.8	0.5	0.8	70
D02	Restricted	0.2	0.2	0.0	13
D03	Private	0.6	0.6	0.8	67
D04	Confidential	0.3	0.3	0.2	27
D05	Restricted	0.8	0.8	0.5	70
D06	Restricted	0.9	0.9	0.9	90

Task c

Risk assessment worksheet (I.e. Risk calculation), including threat and vulnerability assessment (e.g identification and description of each threat and vulnerability for each asset, impact and likelihood of each risk)

- Information Asset Classification (split the consequence + gross risk into another table for readability)

Risk ID	Asset ID	Threat	Vulnerability	Consequence
R01	H01 H03 H04	Theft	Server room location is known to every employee and previously contracted maintenance workers	An attacker breaks into the complex during off hours and steals server hardware.
R02	H07	Theft	Safe contains sensitive documents contains staff information and financial data	Safe is located in the CEOs room, an attacker breaks into the complex during off hours and steals server hardware.
R03	H10	Theft	The NAS drive contains sensitive customer information regarding account data and transaction histories.	The NAS drive is located in the office supply room by the door. An attacker breaks into the complex during off hours and steals server hardware.
R04	H01	Server Hardware Failure	Server could fail and go down for an extended amount of time.	Server failure puts a halt on company processors and directly affects customers causing a disruption of company public image.
R05	H01	Overheating	Server room overheating causing system failure.	Air Conditioning systems could fail causing the server room to overheat, this temperature change could potentially crash the servers network causing business disruptions.
R06	H01 H03 H04 H08	Natural Causes	Smoke detectors batteries are flat and a fire breaks out in the office. Office gets destroyed by an earthquake.	Server room destroyed with everything in it from the switches to routers and servers causing up to $410,000 in damages resulting in huge economic loss for the company.
R07	H01 H03 H04	Overheating , server failure	A disgruntled employee messes with the intelligent airflow in the server room.	Servers start to drop in/out and don’t work as efficiently causing customer dissatisfaction.
R08	H01	Vandalism	A disgruntled an employee or	Huge company economic loss.

	H03 H04		attacker in company off hours breaks into the server room and damages everything in the room.	
R09	H10	Backup failure	The NAS drive becomes faulty and is unable to be used.	Damaged NAS drive potentially causing a loss of important customer data.
R10	H04	DoS	IP fragmentation attack used to bypass the traffic filtering on the router.	An attacker freezes the network by launching a DoS attack onto the company routers.
R11	H04	Session Hijacking	After a session has been established an attacker inserts a falsified IP packet to establish IP spoofing.	Attacker assumes the identity of the compromised user resulting in potential identity theft, information theft and financial theft.
R12	H03	Arp Spoofing	An attacker utilizes the switches associated with the server and executes an arp spoofing attack onto a legitimate user's IP.	After gaining access an attacker launches a man-in-the-middle attack and manipulates a staff member into believing they are the CEO requesting specific information/duties to complete.
R13	H09	Server Failure	The power distribution model fails causing an outage in the office and server room.	Server network goes down and affects customers.
R14	H11	Theft	Staff RFID ID card stolen from an employee.	Unauthorized access to the building.
R15	P03	Theft	There is no screening process for contracted maintenance workers.	The worker steals important equipment and customers/employee documents.
R16	P02	System Failures	Engineers have not been sufficiently trained in handling system duties such as backing up data and ensuring server efficiency.	Backup failures, servers not working up to standard causing customer dissatisfaction.
R17	S01	Firewall Breach	Firewall access has a lack of policies and documentation. Vulnerable to insider attack.	A disgruntled employee messes with the firewall policies making it insecure and open to outsourced attacks.
R18	S02	Malware Injection Attack	An attacker manipulates the hypervisor software and injects malicious code to an entrusted program within	An attacker in the background processors mines sensitive company operational and financial data.

			staff computers.	
R19	S03	Arbitrary Code Execution	An exploit found in Debian 6.0 is in the networking disk cache within google chrome that allowed an attacker to execute arbitrary code execution via crafted HTML page.	An attacker runs RCE (remote code execution) which inputs malware onto the victim's computer allowing for background offline control onto the compromised machine.
R20	S04	Software Failure	Customer management software is outdated and fails.	Loss of customer data or unable to access personal accounts.
R21	D01	Backup failure	The customer management software responsible for saving the week's customer data fails.	Customers are unable to access their account and view their details or transaction history.
R22	D02	Inaccurate Logging	A disgruntled employee edits the stored RFID access logs and unjustly reports them.	Causing workplace tensions and potentially causing a staff member to be unfairly fired.
R23	D03 D04	Inaccurate Logging	A disgruntled employee edits the customer/ employee data profiles.	Disrupts company processors.
R24	D05	Theft	Hired maintenance worker steals the CEOs laptop/harddrive when not present.	Sensitive company financial data and payments are sold to the blackmarket online.
R25	D06	Data Breach	Engineers are not sufficiently trained in handling social engineering attacks and an attacker manipulates the staff into believing they have been sent by the CEO for technical duties.	Unauthorized access to backup data, an attacker could hold the data as blackmail against the company for ransome.

Gross Risk Scoring

Severe	15	19	22	24	25
Significant	10	14	18	21	23
Moderate	6	9	13	17	20
Minor	3	5	8	21	16
Minimal	1	2	4	7	11
	Almost Never	Possible but Unlikely	Possible	Highly Probable	Certain

- Identifying threats and vulnerabilities onto a scale which could pose a risk to business operations at Quantum.

Risk ID	Impact	Likelihood	Risk Rating
R01	Severe	Possible but unlikely	19
R02	Significant	Possible	18
R03	Severe	Possible	22
R04	Significant	Possible	18
R05	Significant	Possible	18
R06	Severe	Almost never	15
R07	Significant	Possible	18
R08	Severe	Possible but unlikely	19
R09	Severe	Possible	22
R10	Significant	Almost never	10
R11	Severe	Almost never	15
R12	Severe	Almost never	15
R13	Moderate	Possible	13
R14	Moderate	Possible	13

R15	Severe	Possible	22
R16	Significant	Possible	18
R17	Significant	Possible but unlikely	14
R18	Severe	Possible but unlikely	19
R19	Severe	Possible but unlikely	19
R20	Moderate	Highly probable	17
R21	Significant	Possible	18
R22	Minor	Possible but unlikely	5
R23	Minor	Possible but unlikely	5
R24	Severe	Possible but unlikely	19
R25	Severe	Almost never	15

Task d

[10] Current and proposed control strategy for each vulnerability/threat/risk, residual risk and the escalation path

- Recommended Risk Controls, applying controls to reduce risks to an organization's assets.

Risk ID	Existing Safeguards	Recommended Controls
R01	- RFID keys cards contain a unique identifier which logs every room each staff member accesses.	- A more in-depth screening process for hired maintenance workers.
R02	- Safe is in the locked CEOs room.	- Use an outsourced safe at either home of the CEO or the bank as the contents will be more secure.
R03	- Employees advised to close the door to the office supply room after use otherwise the door will lock automatically after 1 hour.	- Decreasing the lock timer from 1 hour to around 5 minutes would be more appropriate as the NAS drive is vital for company public image.
R04	- Multiple running servers. - Engineers expected to fix server issues. - Backup every Friday.	- Integrate more servers - Backup data every morning not week.

R05	- Air Conditioning system and power distribution model.	- Include a monitoring system for the air conditioning and in-room server temperatures and notify via an alarm for if any changes were to happen.
R06	- Smoke alarms and distinguishers.	- Ensure smoke alarm batteries are tested/checked and replaced every month or so. - Add external backup components incase of a natural disaster (Safe, NAS drive, customer backup data etc). - Fireproof doors at important locations of the building (server room, CEOs room & office supply room). - Ensure office building is up to current earthquake standards and if not consider moving to a safer building location.
R07	- Assumed workers would not disrupt company operations.	- Add a more in-depth screening process for hired staff members. - Include a temperature monitoring and alarm system in the server room to ensure nothing is failing or tampered with. - Add a “request” function for the server room where an employee must be granted access within reason to enter the server room.
R08	- Assumed workers would not disrupt company operations.	- Add more security to the building. - Make RFID access keys be denied access after office hours unless requested and approved to do so.
R09	- Assumed the NAS drive would not become faulty.	- Routinely change/update the drives to avoid potential damage. - Have a few separate copies of the drive which get updated frequently.
R10	- Assume the router traffic filtering can handle potential IP fragmentation DoS attacks.	- Updating the network firewall rules to ensure protection against IP fragmentation DoS attacks by setting firewall fragmentation rules and inspecting incoming packets that potentially violate these rules, temporarily blocking “unusual” activity.
R11	- Assume the network is protected against session hijacking and the engineers can handle it if this were to happen.	- Ensure company passwords have met the requirements and have 2FA enabled. - Ensuring all software and antivirus is up to date and using a VPN.

R12	- Assumed the switches associated with the servers have sufficient protection against an arp spoofing attack.	- Integrate software dedicated for detecting ARP cache poisoning. - Routinely check ARP tables on devices and set an alarm for suspicious additions or changes. - Arpwatch is a useful tool for continuous network monitoring. - Integrate an Dynamic ARP Inspection (DAI) to the switch boards.
R13	- Assumed hardware failure would not take place.	- Include a monitoring system for the Power DIstribution Model which alerts the engineers if a failure were to take place.
R14	- Assumed the employees would not misplace RFID keys.	- Include a temporarily locking system for RFID key access if misplaced or stolen to ensure unauthorized building access does not occur.
R15	- Assumed hired maintenance workers are up to industry trust standards.	- Include a screening process for hired maintenance. - Add cameras to the important locations in the offices.
R16	- Assumed engineers are trained sufficiently.	- As the hours are quite long for the current engineers it would be best to hire an extra skilled engineer to spread the hours out and ensure they are working to the best of their abilities.
R17	- Assumed the firewall software is up to date and secure.	- Include a monitoring system which notifies the CEO on any suspicious firewall changes or adaptations to avoid potential staffing misconduct.
R18	- Assumed Hypervisor has sufficient security protocols and is up to date on company devices.	- Set access privileges to only trusted individuals. - Create a separate VM from the management network to ensure the company's hypervisor software is secure. - Include server room monitoring and only temporarily granted access to ensure the server's hypervisor is not meddled with.
R19	- Assumed Debian 6.0 is secure and routinely updated.	- As a plentiful amount of Debian 6.0 security issues are related to Chrome browser ensure the company is utilizing safe browning habits and using better browser software such as Brave browser or Firefox.

R20	- Assumed software failure would not take place. - Engineers are expected to check if updates are required.	- Include a notification system to remind engineers and ensure customer management software is routinely updated. - Backup data more frequently in case of customer management software failure.
R21	- Assumed software failure would not take place. - Engineers are expected to check if updates are required.	- Create copies of customer backup data to multiple secure locations in case of software failure.
R22	- Assumed an employee would not disrupt company operations.	- Add cameras to the offices. - Add an alert system which notifies the CEO of any changes to the log files.
R23	- Assumed an employee would not disrupt company operations.	- Same as above, add cameras to the offices. - Add an alert system which notifies the CEO of any changes to the log files.
R24	- CEOs room is locked when the CEO is not present.	- Automatic locking system to important office doors such as the CEOs room. - Camera in CEOs room with smart facial recognition identification software which notifies the CEOs phone of an unknown access.
R25	- Assumed engineers are sufficiently trained and are aware of potential social engineering attacks that could take place.	- Include extensive training on the engineers to ensure social engineering attacks cannot take place. - Implementing an encrypted messaging service such as Signal to ensure potentially breached messaging services are not used.

Conclusion

QuantumNZ like many companies servicing web servers face a multitude of potential risks ranging from physical disturbances (natural disasters) to an attacker breaking in stealing sensitive customer/company data to a remote attacker DoS the servers ultimately taking down the network. Many risks have a severe rating but are quite unlikely to take place. In the event where these could happen there are many ways of which to implement strategies to avoid anything disrupting company operations.

References

Nancy, A., Mukesh, G., Shailendra K.G (2013). *Hypervisor Security - A Major Concern*. Vol 3, No 6, Page 533-538. International Research Publications House.
https://www.ripublication.com/irph/ijict_spl/08_ijictv3n6spl.pdf

(Jan 8th 2019). *How to Perform a Cybersecurity Risk Assessment*. Hashed Out by the SSL Store.
https://www.thesslstore.com/blog/cyber-risk-assessment/

(Aug 13th 2022). *Threats and Attacks on Routers.* Cisco Certified Expert.
https://www.ccexpert.us/scnd/threats-to-and-attacks-on-routers.html

Debian 6.0 Linux Security Risks. CVE-2018-6085. 8.8 Rating
https://vulmon.com/searchpage?q=debian+debian+linux+6.0