Final assignment Fall- 2022-2023

SECURITY

Name: Mahmoud Rumaneh

Id: 20120103

Date: December 22, 2022

Dr. Safaa Hriez

Contents

A.

	Asset name	Why is it valuable?	CIA principles affected
1	Low security (Hardware)	If the devices are not well secured, then anyone can access these devices and destroy it or steal it, so the company will lose the devices and its data, because of that it requires keeping the company, employee, and customer data information more secure for the devices used to work so that the company is not exposed to many financial losses and loss of customer confidence in it.	**Availability:** The device can be destroyed or stolen so the device and its data will be unavailable with no service to give. **Confidentiality:** If the devices stolen then he can see its information.
2	Subnetting (Data and Communication Lines and Networks)	Suppose all devices connect in the same subnet. In that case, if the attacker gets one IP address, all the devices connected to the same subnet will be hacked to get their information and essential data and the attacker can see how many members are in this communication or take the message to send it to another one, change the message if it's not encrypted, or re-order the letters in the wrong order, if the number of devices increases, the amount of traffic on the network increases, which leads to more congestion.	**Availability:** When he destroyed the messages or the data, or deleting the communication lines between the network, or by destroying one device then all devices will be destroyed. **Confidentiality:** When the attacker can read the communication lines messages. **Integrity:** When the attacker can modify the messages or send false messages to the destination.
3	Upload the data by cloud website (Data**,** Software)	The data can be stolen or seen if the attacker made an attack to the data and the website information that he can steal the data during the uploading process to the website and the users in the company won't be allowed to see this data.	**Availability:** The attacker can make the website unavailable from the company side or make the data unavailable by stealing the data or destroy these data during the uploading process. **Confidentiality:** When the attacker can see the data

			during the uploading process. **Integrity:** The attacker can modify the data of the company by changing it during the uploading process to the cloud database servers.
4	Physical access easily. (Hardware, data, and communication Lines and networks**)**	The ability of any person to access Warmaksan's devices and servers exposes it to the risk of stealing the information of employees, customers, and Warmaksan itself, which exposes it to material losses and tarnishing its reputation, by stealing, sabotaging or stealing these devices and data, which causes great harm to Warmaksan.	**Availability:** When the servers and devices stolen or destroyed, use these devices by the attacker to steal and destroy the data, or destroy the communication lines and networks for Warmaksan. **Confidentiality:** When the attacker can see the servers and networking devices' data by seeing the source and the destination of it as seeing the communication lines in Warmaksan. **Integrity:** When the attacker can modify the data of the servers and networking devices or modify the communication lines between the devices in Warmaksan.
5	Servers' room temperature. (Hardware)	If there is nothing to maintain and monitor the temperature and humidity of the data center, it will lead to a rise in temperature due to the work of the servers, causing damage to the ESD and most importantly destroying the servers themselves.	**Availability:** When the devices and servers destroyed or down because of the high temperature.
6	Run applications remotely. (Software, data, and communication lines and networks)	If the employee's device does not contain any anti-virus software, it will be hacked, tampering with his data and affecting his work, and if he forgets his device open in a public place, anyone can access, destroy, modify and steal his data or download malicious programs on his device, which	**Availability:** When the attacker sends viruses to the unsecured employee's device and destroys it or destroys and steals some important data from him, this data will be unavailable.

		exposes Warmaksan's data to danger, so if the device of the remote employee is not properly secured, it may allow attackers to attack Warmaksan's data, so it must be properly secured.	**Confidentiality:** When the attacker or someone see the data of the employee when he left his device open in a public place, or when the employee used untrust VPN software and it was working as Trojan Horse (Malware) to see the data and see the data of Warmaksan. **Integrity:** When the employee left his device open in a public and there was someone who modified his data, or the employee used an untrusted VPN that modified his data and send the wrong data to the Warmaksan network.
7	Third-party access. (Software, hardware)	If the third party uses weak security controls, it becomes more vulnerable to hacking, so the greater the risk of the third party, the greater the risk of Warmaksan, it can be used to hack the third-party system until Warmaksan is affected and hacked as well, where our trust in the third party can be used until the attacker reaches Warmaksan's data.	**Availability:** When the third-party device is destroyed or stolen then he can't support Warmaksan. **Confidentiality:** When the attacker hacks the third-party device and sees data that he shouldn't see it. **Integrity:** When the attacker hacks the third-party device and modify his data or the data of supporting process.
8	Misconfiguration in the network security. (Software, hardware, data, and communication lines and networks)	Misconfiguration causes breaches in the firewall, there are issues with it such as an attacker being able to compromise devices inside the firewall and spirit malware, and websites on the public internet are slowly being accessed by users inside the firewall which causes huge damage for Warmaksan. Also, misconfigured VPN allows attackers to access corporate	**Availability:** When the attackers enter the system easily and destroy important data for Warmaksan, destroy the communication lines by the misconfigured VPN, or destroy software in the devices by malware attacks. **Confidentiality:** The attacker

		resources while appearing to be physically connected to the corporate network, exposing all devices on the Warmaksan's network to threats such as DDoS attacks, malware, and spoofing attacks.	can see the Warmaksan's data easily because the firewall and the VPNs are misconfigured. **Integrity:** The attacker can modify the Warmaksan's data and software easily because the firewall and the VPNs are misconfigured.

B.

Asset name	Threat/ Vulnerability	Existing control	likelihood	Consequence	Level of risk	Risk priority
Low security in the devices	Outside hacker attack	Some of the existing devices are well secured	Possible	Moderate	High	5
Wrong subnetting	Dos, DDos, TCP/IP	Using the password of the employee	Likely	Major	Extreme	2
Using the cloud to upload data	DNS attacks, Website exploit	They are using VPN to connect to the cloud	Possible	Moderate	High	6
No security for the server's room	Internal threats	There's anyone can enter the servers' room	Likely	Catastrophic	Extreme	1
The temperature inside the servers' room	Destroying the servers	Using the servers in short time	Likely	Moderate	High	4
Remote working	Remote access attacks,	Using VPN	Possible	Moderate	High	7

	malware, trojan horse					
third-parties	Malware	Using VPN	Unlikely	Moderate	Medium	8
Misconfiguration on firewalls and VPNs	Malware, remote access attacks	They are using misconfigured firewalls and VPNs	Likely	Major	Extreme	3

C.

Asset name	Suggested countermeasure	How can the suggested countermeasure protect the asset?
Not all existing devices are well secured.	Firewall, antivirus, and password.	When the firewall is activated on all devices, it is very important and is considered the basis of network security because it affects modern and widely used security technologies, it forms a barrier that prevents the entry of unauthorized packets to enter the Warmaksan network and also keeps a record of events that occurred so that administrators can use it to improve the set of security rules. As for anti-viruses, they must be activated on all devices, as they combat any viruses that may attack devices and must always be updated to the latest version, and the password must be set on all devices so that no one can access the device and ensure that every employee has his computer and using a password consisting of uppercase and lowercase letters, symbols and numbers, and not less than 8 digits long.
One subnet is used for all devices	Using VLAN	VLAN is used as a feature to divide the network into multiple subnets as virtual networks and each can have a different number of devices so if one subnet becomes overloaded the other subnets will still be available.
The door was quickly opened	Close the door by password, finger print, or eye scan, CCTV cameras	We should close the door and implement some physical security controls such as passwords, fingerprints, ID cards, or eye scans, all these methods will be given only to the category that can enter the servers' room and prevent unauthorized people.
Using the cloud to upload data	POST, HTTPS	We should use POST commands for communication so that no one can see the data on the website. The data should be stored in the database to

and create accounts		ensure and verify its security standards using tools like Oracle Audit Vault and Database Firewall. In addition to encryption of the data being transferred about customers creating accounts through the web application, it is possible that it is not well secured, so they must ensure that they connect on Hypertext Transfer Protocol Secure (HTTPS). Cameras and video monitoring CCTV to watch and monitor those who attempt to enter one of the doors he is not authorized to enter and hold them accountable.
The temperature inside the servers' room	HVAC System, Netmon	Using the HVAC System (Heating, ventilation, and air conditioning) ensures that the temperature of the server's room is low or in recommended temperature which is between 50 and 82 degrees, using Netmon tool that controls the temperature system by alerts to make sure that the temperature is in the suitable range for the servers and the humidity.
Employees running some applications remotely	Training	By instructing employees on what they should and should not do when working remotely, such as instructing them to open the VPN every time they want to work on the company's network, not connecting to open external networks such as the cafe's network because they endanger the company's data, and installing a VPN and a fire device on their devices.
Grating third-parties to VPN access	Monitor their access	By establishing policies that govern how the third-party handles data and showing them what data, they are authorized to access, in addition to controlling their accessibility and providing them with access to specific data.
Misconfiguration on firewalls and VPNs	Correct configuration and update continually	In order to properly configure firewalls and VPNs as part of the patch management process, it is important to inform employees of the significance of security configurations and how they may impact the organization's overall security. We must also regularly review and update all security configurations in light of new security patches, updates, and notes.

D.

b.

Data protection is a process that shields data or information from detection, destruction, or loss and provides the ability to retrieve the data for use or when I want it because it is important information, which means that the data must be accessible in the event of an event. The more data generated, the more important it is, and we must protect it from corruption or loss, and the more its privacy is protected. Data protection procedures like encryption and backup.

1. General Data Protection Regulation (GDPR): Legislation approved by the European Union on 4 April 2016 and implemented in 2018 unifies EU data privacy law. These instructions focused on increasing data subjects' privacy while maintaining business transparency. If a data breach is discovered, companies must notify all affected parties within 72 hours, according to the GDPR. The instructions in the regulation apply to all data of EU nationals, whether they are in the EU or not, and penalties are set for those who do not comply, with penalties of up to $20 million EU dollars for non-compliance. [1]

The primary goal of the GDRP is to protect the data that describes individuals and thus protect them, as well as to ensure that the organization that collects the data ensures the accuracy of the data and updates it as needed, and to ensure the company's responsibility towards that data. Furthermore, unifying EU regulation is to give EU citizens more control over their personal data and simplifies the regulatory environment for international business. [1]

The regulation requires that personal data be protected from unauthorized processing. It also identified the reasons for collecting personal data and prohibited its use except for a specific purpose and project, as well as setting limits on the amount of data collected, so that only the necessary data for which it is processed is collected. The General Data Protection Regulation establishes several conditions for companies to use a person's Personal Identifiable Information (PII), which is data that can be used to identify a specific person, such as a fingerprint, ID number, email address, and national number, and requires them to meet at least one of the six conditions. [1]

2. Data backup: is a copy of the data that is stored in a different location spare from the original data location. We stored it in another location in the event of a disaster or its destruction, and if I did not backup data and the original data is a disaster, the data may be damaged, and if the data is ruined, I don't have another data, and if I don't have the data, I will lose all the investors, so full backup, differential backup, and incremental backup are all options. [2]

A) Full backup: The full backup is a full copy of data compared to the original data, if we make a full backup for data, every week for example that means Warmaksan should buy space storage each time. But performing a full backup frequently takes a high storage capacity and a long time, so most organizations do it periodically. [2]

B) Incremental backup: Incremental backup is a backup for data but not all data; for example, if I make a backup every day, the incremental backup is just a copy of what changed that day. If I make a backup every week, the incremental backup only copies the data that has changed since the last backup, and this is not a solution for me to include this backup procedure in the Warmaksan. [2]

C) Differential backup: Differential backup is a backup for data that has changed since the last full backup, such as, on the second day I make a backup just for data that changed compared to the last full backup, and on the third day I make a backup just for data that changed compared to the last full backup, which means I make a backup for data that changed in the second and third days (the days after the full backup day), and this is a good solution to Warmaksan to make a backup. [2]

3. Data Encryption: Encryption is the process of converting plaintext (readable data) into ciphertext (unreadable data) using a mathematical algorithm called a "cipher." The ciphertext can only be read by someone with the proper decryption key, which is used to reverse the encryption process and convert the ciphertext back into plaintext. [3]

There are two main types of encryptions: symmetric and asymmetric.

Symmetric encryption uses the same key for both encryption and decryption. For example, a sender could encrypt a message using a secret key, and the recipient could decrypt the message using the same key. [3]

Asymmetric encryption, also known as public-key encryption, uses two different keys: a public key and a private key. The public key is used to encrypt the data, and the private key is used to decrypt it. Anyone can use the public key to encrypt data, but only the person with the corresponding private key can decrypt it. This method is commonly used for secure communications, such as in HTTPS and VPNs. [3]

Encryption is a security measure that is used to protect sensitive data from unauthorized access. It is used in a variety of contexts, including protecting data in transit (such as when it is sent over a network), protecting data at rest (such as when it is stored on a hard drive), and protecting data in use (such as when it is being processed by an application). [3]

E.

Risk Assessment: A specialized person performs risk assessment, which is the identification of hazards that would negatively impact a Warmaksan's ability to conduct business. Determine the methods to be used in order to eliminate or control risks. These assessments aid in identifying inherent business risks and providing measures, processes, and controls to reduce the impact of those risks on business operations. A hazard is anything that can cause harm, such as workplace accidents or toxic chemicals. The risk is the possibility of damage being caused. And part of any assessment plan is defining the hazard and then calculating the likelihood of the hazard occurring. [4]

The goal of risk assessment is to help organizations prepare for and combat risk, meet legal requirements, raise awareness about hazards and risks, and create an accurate inventory of accessible assets. [5]

There are five steps in the risk assessment process:

1. Identify the hazards: The first step we should know what hazards our employees and Warmaksan face including: Phishing, Malware, Device vulnerabilities, Web Application vulnerabilities as I mentioned here (B).

for Web Application vulnerabilities...

Warmaksan's web applications are vulnerable to a number of different attacks. These include SQL injection attacks, cross-site scripting attacks, and session hijacking. Additionally, Warmaksan's web applications are not properly encrypted, which means that sensitive information such as passwords and credit card numbers could be compromised. [5]

2. Determine who might be harmed and how: After identifying each dangerous step in the first step, consider who will be harmed if the danger occurs. For the Web Application, vulnerabilities hazard the customer and employee will be harmed. [5]

3. Evaluate the risks and take precautions: Now I actually have a listing of potential hazards; thus, I want to think about how seemingly it's that the hazard can occur and the way severe the results are going to be if that hazard occurs. This analysis will facilitate me to verify wherever I ought to scale back the amount of risk and which hazards I should rank first. as I mentioned here (B). [5]

4. Recording my findings: The results of the risk assessment must be formally recorded by Warmaksan, my plan should include the hazards I've found, the people they affect, and how I plan to mitigate them. The risk assessment plan should show that: Conducted a look at my workspace, determined who could be affected, controlled and handled apparent risks, initiated precautions to keep dangers low, and kept my teammates involved in the process. [5]

5. Review assessment and update if needful: The workplace is usually changing, and the risks of Warmaksan change as well. As new equipment, methods, and folks are introduced, each brings a new hazard. I'll frequently review and update my risk assessment process to remain in the prime of those new hazards, and stop or reduce them. [5]

H.

Security policy is a set of roles the organizations have to follow, we have to create a security policy for Warmaksan, to find out who is harming Warmaksan and they are members of the company or competitors. The goal of security policy is to Warmaksan protect Confidentiality, Integrity, and Availability. (C.I.A), we have many policies that I will use for Warmaksan, such as VPN and firewall, data backup, physical access control, password, third party, and remote access policies:

1. VPN and firewall:

Scope: Warmaksan's employees.

Policies:

a. Clearly define the security policy and objectives for the firewall and VPN, including the types of traffic that should be allowed or blocked.

b. Configure access control rules on the firewall to allow or deny traffic based on source and destination IP addresses, ports, and protocols.

c. Test the firewall and VPN to ensure that the configuration is working as expected and that all security policy rules are being enforced.

d. Regularly update and patch the firewall and VPN software and firmware to ensure that the latest security features and fixes are in place.

e. Regularly review and audit firewall and VPN policies and configuration, including access controls, to ensure they are still aligning with the Warmaksan's security needs.

f. Train employees on the use of firewall and VPN.

g. Identify and segment different networks, such as internal, DMZ, and external networks, to ensure proper security controls are in place.

2. Data backup:

Scope: Warmaksan' data such as database, user and employee information.

Policies:

a. Determine what data needs to be backed up (sensitive data), how often it should be backed up (every day, deferential backup), and where the backups will be stored (cloud).

b. Using the son-father-grandfather approach in the backup.

c. Using Adopting General Data Protection Regulation (GDRP) to protect the personal information of Warmaksan's users

d. Set up a schedule for regular backups to ensure that all important data is saved and up-to-date.

e. Periodically test and verify the backups to ensure that they can be successfully restored in case of a data loss.

f. Keep a copy of the backups in a secure location (hot site) away from the main data center to protect against physical disasters.

g. Review and update the backup policy regularly to ensure it stays current with the organization's needs and security standards.

h. Encrypt the data before backup

i. Regularly test the restore process to ensure that the backups are valid and can be used in case of disaster recovery.

j. Store multiple copies (3 copies) of backups in different locations to ensure redundancy and availability. (I will keep it external in hot site)

k. Use backup software that can provide versioning and incremental backups, this will allow you to restore files or folders to a specific point in time.

l. There must be a watermark on the data to preserve the company's ownership of it.

m. When backing up, I should process the backup during non-working hours, like holidays such as Fridays and non-working hours, so as not to affect your company's work.

n. Reducing the accessibility of it by employees and allow some reliable members of staff to arrive for backup.

3. Physical access control:

Scope: All employee that can enter the data center.

Policies:

a. Identify the individuals or groups who are authorized to enter Warmaksan.

b. Establish procedures for granting and revoking access, such as background checks, fingerprints, or ID cards.

c. Implement physical security measures, such as locks, CCTV cameras, and alarm systems, to prevent unauthorized access to the Warmaksan.

d. Regularly review and update the access control policy and procedures to ensure they remain effective.

e. Regularly audit and monitor the access control system to detect and prevent any unauthorized access attempts.

f. Document all access attempts and any security breaches, and maintain records for compliance and incident investigation.

4. Password:

Scope: All employees in Warmaksan, third parties and customers.

Policies:

a. Establish minimum requirements for password complexity, such as a minimum length, and the use of uppercase and lowercase letters (a-z, A-Z), numbers, and special characters (@#$%! *&%^.,)(‘[];).

b. Require employees to change their passwords regularly, every month.

c. Encourage employees to use of a password manager to generate and store complex passwords.

d. Don't use of easily guessed or common words, such as "password" or "1234," as well as personal information.

e. Prohibit the sharing of passwords, and employees are required to keep their passwords confidential.

f. Password reuse is not allowed. The password must not be the same as the last 5 changes made to the same employee in Warmaksan.

5. Third party:

Scope: third party support.

Policies:

a. Documenting any incidents or violations of the third-party policy and reporting them to the appropriate parties within the organization.

b. Enter limits for the third-party connections.

c. The third-party mustn’t have an access to the customer personal information or the sensitive data in Warmaksan.

d. Identifying potential third-party partners and evaluating the potential risks associated with each one.

6. Remote access:

Scope: Remote access employees.

Policies:

a. Identifying the types of remote access that will be allowed and evaluating the potential risks associated with each one.

b. creating technical controls such as firewalls, VPNs, and multi-factor authentication to protect remote access connections and ensuring that all remote access devices meet security requirements.

K.

The roles of stakeholders in Warmaksan to implement security audit recommendations are:

1. Management: playing a key role in implementing security audit recommendations by allocating resources such as personnel and funding, to implement the security audit recommendations, developing and implementing a plan of action, coordinating with other departments like communicating the security audit recommendations to the board of directors and working with them to develop an implementation plan, monitoring progress, and communicating with the board of directors and the stockholders. [7]

2. IT officers: IT officers are responsible for ensuring that technical controls and security measures are in place to protect the company's assets and information when implementing security audit recommendations. Furthermore, IT officers must assess the current technical controls and security measures in place to identify any gaps or vulnerabilities that must be addressed. IT officers are also in charge of configuring and maintaining security systems, as well as keeping them up to date with the latest security patches and software. [7]

3. Risk owners: As a stockholder, the risk owner's role in implementing security audit recommendations is to ensure that Warmaksan's assets, including financial and personal data, are safeguarded against potential threats such as cyberattacks. This could include reviewing and approving security audit recommendations, allocating resources to put them into action, and monitoring their effectiveness. Furthermore, they must ensure that the company complies with all applicable data protection and security laws and regulations. The ultimate goal of the risk owner is to act in the best interests of the company and its shareholders by minimizing potential risks and protecting Warmaksan's assets. [7]

4. Facility and security: As stockholders, the facility and security roles in implementing security audit recommendations typically entail ensuring the physical security of Warmaksan's facilities and assets. This could include putting in place measures like surveillance systems, access controls, and emergency response plans. Security personnel, such as security guards or consultants, may also be chosen and overseen by stockholders. They may also be in charge of allocating funds for security-related expenses such as equipment, training, and maintenance. The goal of these positions is to protect the company's facilities and assets from potential security threats like theft, vandalism, or unauthorized access. [7]

5. Risk and Compliance: Stockholders' risk and compliance roles in implementing security audit recommendations typically involve ensuring that Warmaksan is adhering to relevant data protection and security laws and regulations, as well as minimizing potential legal and financial risks to Warmaksan. This could include reviewing and approving security audit recommendations, monitoring compliance with relevant laws and regulations, and ensuring Warmaksan have adequate policies and procedures in place to protect sensitive information. They may also be involved in the hiring and supervision of compliance and risk management personnel, as well as the allocation of resources for compliance-related expenses. The goal of these roles is to ensure that Warmaksan follows industry standards and regulations, to reduce potential legal and financial risks, and to protect Warmaksan and its shareholders from potential penalties or loss. [7]

References

[1] Castagna, R. and Lavery, T. (2021) What is GDPR? an overview of GDPR compliance and conditions, WhatIs.com. TechTarget. Available at: https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR (Accessed: January 1, 2023).

[2] Wallen, D. (2020) Types of backup: Full, differential, and incremental, Spanning. Available at: https://spanning.com/blog/types-of-backup-understanding-full-differential-incremental-backup/#:~:text=There%20are%20mainly%20three%20types,full%2C%20differential%2C%20and%20incremental (Accessed: January 1, 2023).

[3] Forcepoint. 2022. *What is Data Encryption?*. [online] Available at: <https://www.forcepoint.com/cyber-edu/data-encryption#:~:text=Data%20encryption%20is%20a%20security,or%20entity%20accessing%20without%20permission> (Accessed 2 January 2023).

[4] SearchCompliance. 2022. What is a Risk Assessment? - Definition from WhatIs.com. [online] Available at: <https://searchcompliance.techtarget.com/definition/risk-assessment> (Accessed 3 January 2023).

[5] Lucidchart.com. 2022. A Complete Guide to the Risk Assessment Process | Lucidchart Blog. [online] Available at: <https://www.lucidchart.com/blog/risk-assessment-process> (Accessed 5 January 2023).

[6] Pecb.com. 2022. ISO 31000 Risk Management - Training Courses & Certification - EN | PECB. [online] Available at: <https://pecb.com/en/education-and-certification-for-individuals/iso-31000> (Accessed 8 January 2023).

[7] Liquori, T., 2022. What Is the Ideal Server Room Temperature? | Learn More. [online] Dataspan. Available at: <https://dataspan.com/blog/what-is-the-ideal-server-room-temperature/> (Accessed 12 January 2023).