

Security

10203280

D/618/7406

Section (8)

Submitted to

Dr. Heba Al-Alawneh

Submitted by

Nasrullah Rami Alhaj Hamad

1. **Discuss the most critical assets of the Warmaksan's system, considering their CIA principles in mind.**

|  |  |
| --- | --- |
| **Asset Name (including the CIA)** | **Justification for why it’s critical** |
| The integrity and confidentiality of customer data | Customer data is set to be the biggest priority in the company because of its reputation, failing to protect customer data from getting altered by unauthorized individuals would destroy the company. |
| Availability and confidentiality of the endpoints within the network | All devices should be well-secured and be able to face any attacks such as malware. Otherwise, attackers can easily attack the employees’ laptops |
| The authenticity of the employee endpoint devices across the branches of Warmaksan | This asset is important in every company because it ensures that the employees are not being spoof-attacked and are trustworthy to do their tasks |
| Reliability and confidentiality of the server room | The room that carries the database and the print servers should be well secured by multiple security protocols such as CCTV and a secure door, to prevent any unauthorized access to the data center. It should be reliable enough to secure the data. |
| Accountability and confidentiality of the cloud system that carries customer information | The cloud system should be accountable for any loss in customer data sent by Warmaksan. Since it is private data that isn’t available to anyone. |
| Reliability and availability of the services and the applications within the company | The services used in the company must be well-secured and reliable by implanting antiviruses. So, they don’t steal employee data or damage the software. |
| Reliability of the network connection that will be used to upload the data of each branch to the cloud system | The internet connection used in uploading the data should be safe inside copper wires. So, it can be reliable when the data from branches is passed on the cloud system. |

1. **Suggest (given the notes above) the possible controls/countermeasures initially used by the company to protect their asset.**

|  |  |
| --- | --- |
| **Asset Name (including the CIA)** | **Controls initially used by the company** |
| The integrity and confidentiality of customer data | Customer data is kept safe in servers in the data center |
| Availability and confidentiality of the endpoints within the network | Some endpoint devices were secured |
| The authenticity of the employee endpoint devices across the branches of Warmaksan | Password policy was used for the devices |
| Reliability and confidentiality of the server room | The server room is protected by a secure door, a fire alarm, and CCTV cameras |
| Accountability and confidentiality of the cloud system that carries customer information | No Controls |
| Reliability and availability of the services and the applications within the company | Most of the services and applications are well-secured by security protocols and software |
| Reliability of the network connection that will be used to upload the data of each branch to the cloud system | The network connection will be provided and secured |

1. **Discuss and assess the Warmaksan system's possible risks, their likelihood (rare, unlikely, possible, likely, and almost certain), and exploitation consequences (insignificant, minor, moderate, major, catastrophic, and doomsday).**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset Name (including the CIA)** | **Possible Risks** | **Impact** | **Likelihood** | **Justification for likelihood and impact** |
| The integrity and confidentiality of customer data | Customer data getting stolen or altered by attackers by MiTM attacks | Doomsday | Likely | Losing customer data could cause disastrous problems for the company and its reputation. It’s likely to happen since no proper controls are initiated in the data center. |
| Availability and confidentiality of the endpoints within the network | Endpoints getting attacked by ransomware from threat actors | Catastrophic | Possible | Security protocols not existing within the endpoints can result in the loss of the data inside each endpoint. But some of the endpoints were secured the likelihood is possible |
| The authenticity of the employee endpoint devices across the branches of Warmaksan | Employee identity and sensitive information stolen and altered | Catastrophic | Possible | If employees lose their identities sensitive data can be stolen. It is possible to happen because of password policy issues. |
| Reliability and confidentiality of the server room | Unauthorized access to the data center | Catastrophic | Likely | Losing the data from the database is dangerous and could guarantee bankruptcy for the company, and it’s likely to happen because the control inside the data center is poor |
| Accountability and confidentiality of the cloud system that carries customer information | Major financial losses and theft of private customer data | Catastrophic | Possible | The cloud system should be accountable for any loss in customer data, and the risk is possible because there are no controls initiated. |
| Reliability and availability of the services and the applications within the company | Employees are vulnerable to attacks, and sensitive data available to unauthorized sources | Moderate | Likely | Viruses planted in the devices lead to a loss in availability only. Therefore, the impact could be moderate, and it’s likely to happen because the company has its services and applications unpatched. |
| Reliability of the network connection that will be used to upload the data of each branch to the cloud system | DNS or TCP/UDP spoofing attacks, other Internet-related attacks | Major | Likely | The process of uploading the data is seen as a vulnerability by attackers, spoofing attacks would be done which causes a loss of authenticity. It’s unlikely to happen because the network connection is secured |

**Final Risk Registry:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Asset Name (including the CIA)** | **Possible Risks** | **Existing Controls** | **Impact** | **Likelihood** | **Risk Level** | **Priority** |
| The integrity and confidentiality of customer data | Customer data getting stolen or altered by attackers. | Customer data is kept safe in servers in the data center | Doomsday | likely | Extreme | 1 |
| Availability and confidentiality of the endpoints within the network | Endpoints getting attacked by ransomware from threat actors | Some endpoint devices were secured | Catastrophic | Possible | Extreme | 4 |
| The authenticity of the employee endpoint devices across the branches of Warmaksan | Employee identity and sensitive information stolen and altered | Password policy was used for the devices | Catastrophic | Possible | Extreme | 3 |
| Reliability and confidentiality of the server room | Unauthorized access to the data center | The server room is protected by a secure door, a fire alarm, and CCTV | Catastrophic | Likely | Extreme | 2 |
| Accountability and confidentiality of the cloud system that carries customer information | Major financial losses and theft of private customer data | No Controls | Catastrophic | Rare | High | 5 |
| Reliability and availability of the services and the applications within the company | Employees are vulnerable to attacks, and sensitive data available to unauthorized sources | Most of the services and applications are well-secured by security protocols and software | Moderate | Likely | High | 6 |
| Reliability of the network connection that will be used to upload the data of each branch to the cloud system | DNS or TCP/UDP spoofing attacks, other Internet-related attacks | The network connection will be provided and secured | Major | Unlikely | High | 7 |

1. Recommend ways to improve Warmaksan's IT security via:
   1. Describe and assess different security controls that could be applied to protect the most critical assets (customers & business-critical data)

|  |  |
| --- | --- |
| **Critical Asset Name (including the CIA)** | **Controls to improve security** |
| The integrity and confidentiality of customer data | -Limit the number of employees with access to the data center  -Implement regulations when dealing with sensitive data, like customer data. |
| Availability and confidentiality of the endpoints within the network | -Installing and configuring antiviruses and firewalls.  -Train employees for attacks or threats |
| The authenticity of the employee endpoint devices across the branches of Warmaksan | -Update the password policy.  -Train employees on authentication  -Limit the number of employees authorized to access data |
| Reliability and confidentiality of the server room | -Update the fire alarm  -Control the temperature in the servers’ room  -Fix the data center door.  -Implement CCTV cameras.  -Use digital prints like fingerprints or face IDs for employees when entering the data center |
| Accountability and confidentiality of the cloud system that carries customer information | -Choose a safe reliable cloud system  -Force the system to take accountability when carrying customer data.  -Make backups of customer data, in case it got lost in the cloud system |
| Reliability and availability of the services and the applications within the company | -Install security protocols inside the services.  -Patch any bugs the company applications carry and fix them  -Make sure customer services are available for the customers |
| Reliability of the network connection that will be used to upload the data of each branch to the cloud system | -Have a backup internet connection in case it was cut out  -Use a wired connection for Wi-Fi because it guarantees safety and saves a lot of time. |

|  |  |
| --- | --- |
| **Recommended controls to protect customers** | -Limit access to employees to customer information, so when they are implemented, the risk becomes low, which increases the protection of data.  -Implement policies and authentication protocols for customers, to prove that the person is the owner of the data. By implementing two-factor authentication. |
| **Recommended controls to protect business-critical data** | -Backup business data daily, to make a copy of the data and store it in a secondary location to save it in case of losing the original data. This is a key component of the DRP and the BCS.  -Encrypt the business data on a regular basis, so that people who have access to the decryption key can read and translate |

* 1. Explain data protection processes and regulations that might enhance Warmaksan's IT security.

Processes can be either by protecting the data or backing up the data,

Data Protection: can put the data at rest, which includes any stored data and hardware storage devices like hard drives and mobile phones.

Data Backup: Can be done by making extra copies of the data for the purpose of restoring the data in case of damage.

There are many regulations related to data protection such as:

GDPR (General Data Protection Regulation) (2016/18)

GDPR is a European Union law that was adopted on the 14th of April 2016, it was enforced on the 25th of May 2018. It was created to give control to individuals over their personal data and address the processing of the personal data of people that live in EEA. It can be applied to any company in any country or location, regardless of the citizenship of the individual.

The processors or the company management should put appropriate technical and organizational measures to implement the data protection principles that will be used within the company. The processes that handle personal data should be built into consideration with the principles and must provide safeguards to protect data.

The systems must be designed with privacy as a priority, by using the highest possible privacy settings. The datasets cannot be publicly available and aren’t used to identify an individual

Personal data can’t be processed if they’re consent, contract, public task, vital interest, legitimate interest, or legal requirement.

The data must be disclosed to other parties, and any sharing of data with third parties or organizations outside of the company must be stated beforehand.

Subjects have the right to have their data erased under certain circumstances and they may request and be provided a portable copy of their data.

* 1. Analyze the IT security audit and its impact on Warmaksan IT security.

|  |  |
| --- | --- |
| **IT Security Analysis** | Starting with the endpoint devices that lack security in the network, can be solved by installing antiviruses and configuring firewalls, and they all are connected to one subnet which indicates that there’s high traffic but can be fixed by implementing multiple subnets one for each continent for example. The employees in Warmaksan use a password policy with issues that should be fixed by issuing a new password policy. Some employees have access to the data center remotely which should be limited, some third parties have VPN access to the data center too but for support reasons and they should be accountable for any loss. The door that leads to the data center can be quickly opened, which means there’s low security for the servers and networking devices inside, it should be fixed and several security protocols like digital prints, the server’s room has poor temperature and humidity control, which should be handled immediately to prevent servers from malfunctioning and the system itself has auditing issues, which can be fixed by following a standard regulation. The infrastructure is proper for protecting customer data, but the controls initiated are weak and not strong enough to handle data loss or attacks in the future. |
| **Security Audit impact** | Following a security audit can benefit Warmaksan a lot. Since most audit benefits include data protection measures by encryption use and network access control, which can fix the problem the data center is facing with low controls. Some audits also perceive functioning from a different view, by examining the network infrastructure of Warmaksan, to provide the knowledge required to optimize their security and their business. Auditing can also point out the vulnerabilities in a system to prepare for future encounters and to prepare the best approach when solving a risk. Auditing can help make anyone responsible for their actions in Warmaksan, this will aid the company, especially with its transformation to the cloud, since a lot of third parties can steal information and be known as untrustworthy, having an audit can help prevent them from stealing and make them accountable for their actions. Auditing can save money and help evaluate security policies; the company needs to improve its policies because some of them have issues. Lastly, having an audit can assist in noticing any misuse of resources inside the company and preparing for improvements. |

1. Review the risk assessment procedures in Warmaksan

|  |  |
| --- | --- |
| **Security Risk Assessment Approach** | Combined. Since it includes all the other approaches, to provide protection as quickly as possible in Warmaksan. It starts with implementing baseline security recommendations on all systems, then systems exposed to high-risk levels are identified at a higher level in the risk assessment. An informal risk assessment gets directed on key systems by a decision. Lastly, a full detailed risk analysis can be conducted. This results in implementing the most appropriate controls as fast as possible. |
| **Acceptable Risk Level** | Medium. Because most of the possible risks Warmaksan could face are on the high-extreme side, which cannot be acceptable since it can destroy the company. |
| **Risk Assessment Type** | Qualitative risk assessment, because the company has a lot of branches, and it is easier to calculate the scale of the attack and the cost of recovery. It aims to calculate the scale of the impact and the likelihood, based on which the best cause of action will be chosen. |
| **Risk Assessment Process (In steps)** | -1 Prepare for Assessment: We first need to explore the organization’s environment, Warmaksan is a company that is less vulnerable to threats since it has a big reputation of security and protecting its customers from attackers, the management decided to transfer all the data across a cloud system for better security and better performance for the traffic. The management has decided to accept the risk if it’s at the medium level and eliminate any risk that levels threaten the assets. Using the combined approach, and the implementation of multiple policies, the assets that need to be protected in the organization are the following:  a- Hardware assets, such as endpoint devices, and servers.  b- Software assets, such as security protocols, and VPN.  c- Information assets, such as customer data and financial information.  -2 Conduct Risk Analysis: After we have determined the critical assets in the organization, we must identify the threats and their sources, the vulnerabilities, the likelihood of the threat, and the impact.  The threats are Viruses, Malware, Ransomware, and MiTM attacks.  The threat sources for the threats above are man-made, and viruses can be accidental.  The vulnerabilities inside the company can be poor control of the data center security, issues with the password policy, issues with the auditing policy, loss of security protocols in endpoint devices.  The likelihood can be determined based on the controls initiated by the company and how far the vulnerabilities are exposed, which can be considered likely and almost certain. The impact can be catastrophic, doomsday, and major, which is determined by the controls initiated and how much the threat threatens the company and its vulnerabilities.  -3 Communicate Results:  The risk registry above can determine risk level, whether high or extreme, which cannot be acceptable to Warmaksan, so it must be eliminated and taken care of, by implementing several proper controls that can protect the assets and the company from risks and potential threats, and training the employees to handle risks and getting in touch with the senior management of Warmaksan to convince them to set up the risk assessment mentioned above. So, they can implement it correctly for more performance.  -4 Maintain Assessment: By implementing the controls needed to defend against threats and potential attacks, the risk assessment is proved as a success, but proper actions must be made so it maintains the process of protecting the company from risks, such as regular maintenance for the company, incident handling and getting rid of risks, a change in management every once in a while. |

1. Explain how you can benefit from an appropriate risk management approach or ISO risk management methodology by summarizing it and highlighting its application in the IT security of this project.

The ISO risk management system was made by iso (International Organization for Standardization) to provide recommendations for risk management to enterprises, the risk management process it follows consists of six different steps which are:

Risk Identification: this identifies the obstacles that would stop organizations from reaching their goal

Risk Analysis: This identifies the causes of the threats that were found in the organization.

Risk Evaluation: It determines if the risk is reasonable by comparing the risk analysis results to risk criteria.

Risk Treatment: This changes the positive and negative immensity of the likelihood of the impacts that fall on the organization.

Establishing the context: The scope of the process and the organization’s objectives should be defined, whether external (Stakeholder expectations) or internal (Culture).

Monitoring and Review: Used to compare the risk assessment performance and the measures in organizations.

Communication and Consultation: Aids in understanding the stakeholders’ interests and ensuring that the process is explaining the reasons for decisions and risk treatment options.

The benefits of ISO 31000 occur in organizations as the following:

* It gives Warmaksan a competitive advantage: Since it’s a recognized standard, it increases customer confidence in Warmaksan, which raises the competitive level locally and globally.
* Raises employees’ awareness of risks: By educating employees in Warmaksan about the risks that it might face, risks can be reduced and eliminated.
* Increase Investor Confidence: By showing responsibility for risks and reporting them and trying to reduce them, Warmaksan investors will have increased confidence.
* Improving Warmaksan culture: By bringing departments together to share new views and consider how to work together more efficiently.
* Improving the success rate of all processes and decisions: By focusing on the process instead of waiting to be reactive
* Prepare the business for all eventualities: By understanding the expected worst-case scenario, and making use of resources and opportunities currently available

1. Discuss, in detail, the security impact of any misalignment of IT security with Warmaksan policy and recommend how to maintain their alignment

Security misalignment happens when the CISO and the CIO have competing priorities that might separate them rather than align them toward common objectives, and every company uses its own set of policies. If the IT security policy exists, then the organizational policies are present

The impact of any misalignments of security can be described as a conflict in the system which would lead to exposure in the system. It can also lead to employees not knowing what to do when following policies, especially if the misalignment blocks the policy that isn’t meant to be blocked. It can also result in the destruction of the system’s security, making it simple to breach.

Which can also lead to a loss of private data in the data center and servers. While destroying the company’s reputation.

Prevention of such misalignments can be done by maintaining the business safe from harm and protecting the customers, workers, and policies from any threat, and protecting both customer and corporate data from any attacks in the most fundamental way possible.

Fundamentally, a misalignment is when the management that is responsible for making policies has a contradiction for the IT department.

An example would be management allowing the employees to use youtube but the IT department banned it from being opened on the network. This causes confusion for the employees.

1. Design a suitable security policy for Warmaksan, including the main components of an organizational disaster recovery plan.

Information security policies have three essential types that are used in companies, to ensure that employees are aware of attacks and achieve security. These types are:

* Enterprise Information Security policies: These specialize in setting up rules to protect programs. For example, The Disaster recovery plan.
* Issue-specific Information Security policies: These policies focus on everything that has to do with employees and their connection to the devices. By issuing rules when dealing with devices or using them.
* System-specific security policies: They focus on the systems of the company and work on protecting them with a set of rules. For example, tools I used for the system security policy, SIEM and SOAR

The Disaster Recovery Plan (DRP): is a set of rules that organizations must follow if a crisis happens, either natural or man-made. So critical data and other assets can be recovered, this plan contains many essential components such as:

1. The DRP team, which consists of expert individuals each in a different area, and is responsible for the implementation of the plan.
2. Recovery Time Objective (RTO): This is the amount of time that the company needs to be restored, the time chosen should be realistic and based on the consequence of the risks.
3. Recovery Point Objective (RPO): RPO is the maximum amount of critical data that can be lost in a crisis, this component can ensure proper recovery of data while preventing data loss.
4. Backups: backups are essential for recovery after each crisis, so it saves time when recovering them. Backups also allow access to data if a system goes down.
5. Documentation: The plan should be well documented, so employees and the company can follow it easily after a crisis. Without documentation, the plan may not be followed properly as intended.

|  |  |
| --- | --- |
| Policies are a set of rules that influence decisions, and they must be read and understood and agreed-to to be functional. Policies are issued by senior management, and the policies included in Warmaksan were the following:  **-Password policies:** a set of rules that determine the users a course of action when choosing a password.  **-Email Policy:** a policy that a business might implement so the employees can use emails in a more efficient way while keeping their identity and data protected  **-Access Control Policy:** a policy that specifies how access should be managed and who can access the data under different conditions  **-Data protection Policy:** a policy that focuses on handling the data and managing it, with the main goal being securing all the information. | |
| **Included Policies** | **Justification for the Included Policies** |
| Password Policy | This is essential in the company to protect the authenticity of the endpoint devices and because there are already issues with the already implemented policy |
| Email Policy | Because it prevents security breaches and works on keeping the employees within the reach of their organization and is aligned with the aim of the business |
| Access Control Policy | This policy is important because Warmaksan must limit employee access to the data center, especially after implementing new controls. |
| Data Protection Policy | This policy is very essential, especially after moving the information to a cloud server, a new policy should be implemented focusing on how data should be handled and managed and what data shouldn’t be used in any sort. |

1. Automation: This helps save time and effort when implementing the DRP by speeding up the process of recovery and ensuring that all the steps are well-taken. It also helps reduce human-error during the DRP process.

1. Justify the developed security plan, giving reasons for the elements selected.

|  |  |
| --- | --- |
| **Included Policies** | **List of sub-policies** |
| Password Policy | -Passwords must be from 8 to 64 characters long  -Passwords must be changed every 6 months  -Passwords must contain special characters and numbers |
| Email Policy | -Emails cannot contain ALL-CAPS  -Emails mustn’t be used for harassing or threatening others  -Emails from unknown sources mustn’t be opened |
| Access Control Policy | -All users must use the digital print to access the data center  -The users must leave after 15 minutes of inactivity  -Passwords should be provided for a two-factor identification |
| Data Protection Policy | -Data should be backed up regularly every day.  -Sensitive data should be protected heavily inside the servers.  -Customer data should be disclosed to other parties. |

1. **Evaluate the suitability of the tools used in this policy.**

|  |  |
| --- | --- |
| **Tools used within the policy** | **The Evaluation of the Tool** |
| Firewall Systems and IDPS | Firewalls and IDPS can deny or allow access to different users, if configured correctly, they can prevent unauthorized parties access to the software system, which also helps with data protection. On the other hand, firewalls can’t be used for password or email policies. The firewalls should be updated to the new-generational firewalls IDPS Firewalls. |
| Digital Print (Two-Factor Authentication) | Digital prints can be used for two-factor authentication which enhances the security of the data inside the data center, and it can be used in the data protection policy as well as the access control policy, but it can’t be used in the Email policy or the password policy |
| CCTV Cameras | These cameras are used to identify anyone who enters the data center. It can be used in both the data protection policy and the access control policy, but it can’t be used in the password policy and the email policy. |
| Security Information Event Management and Security orchestration, Automation, and Response (SIEM and SOAR) | **SIEM** is a tool used in the enterprise companies to provide regular reporting and analysis of the security events, the systems must include functions like:  **Forensic analysis** searchs logs and records from sources.  **Correlation** examines the logs from systems and speeds the detection of the threats.  **Aggregation**: reduces the volume of the data by consolidating duplicated records  **Reporting:** Presents the correlated data in regular monitoring and summaries.  SIEM provides information on the suspicious activity source such as their name and location, their device information, and posture information such as the compliance of the device with the policy.  **SOAR** is used to enhance the SIEMby helping teams investigate incidents by gathering functionalities that aid in incident responses.  SOAR provides case management tools that allow cybersecurity officers to research and investigate incidents, by integrating threat intelligence into network security. And uses AI to detect incidents that aid in analysis, it also automates complex incident response procedures, and offers dashboards and reports to document incident response so they improve their performance and the network security. |

1. A discussion of the roles of stakeholders in the Warmaksan to implement security audit recommendations.

The stakeholders in Warmaksan are the people responsible for the management, implementation of security controls and policies, and protection of data, and there are many stakeholders in Warmaksan, such as:

* **The Management**: This ensures that the audit recommendations are implemented in Warmaksan effectively and in a timely manner. The management also ensures that the resources needed for the recommendations are available and ensures the implementation doesn’t affect the business.
* **IT Offices**: They ensure that the security measures are implemented correctly and are responsible for the recommendations by the security audit, they make sure the implementations don’t impact the performance of the system negatively.
* **Risk Owners**: are responsible for reducing any risks connected to the vulnerabilities identified by the audit, they also associate with the management and IT offices to implement the needed features and ensure that the risks are acceptable
* **Facility and Security:** they ensure the physical security implementation and measures’ placement and the security of the data center of Warmaksan.
* **Risk and Compliance:** They are responsible for the compliance of Warmaksan with the audit recommendations, and they associate with all of the other stakeholders to ensure the measures are implemented and that Warmaksan is compliant.

**Reference:**

1. *Managing risks and risk assessment at work* (no date) *HSE*. Available at: <https://www.hse.gov.uk/simple-health-safety/risk/steps-needed-to-manage-risk.htm> (Accessed: January 31, 2023).
2. *Security policy templates* (no date) *Information Security Policy Templates | SANS Institute*. Available at: <https://www.sans.org/information-security-policy/> (Accessed: January 31, 2023).