Risk Management Case Study

Executive Summary

DHAEI has requested that during this crucial time in their development and expansion that we take a look at their business operations, and perform a risk analysis report. DHAEI has provided us with the company infrastructure of associates, senior associates, managers, and executives. Along with this information was the infrastructure of the network, how many devices are connected to the network, and finally the planned changes to their infrastructure.

1. Purpose, scope, and users

The purpose of this document we will be able to categorize the risks that are involved with the company, the risk owners responsible for those risks, as well as the impact that the risks could have if they are compromised by malicious attackers. After categorizing the risks this document will then proceed to list the mitigation or treatment methods that could be implemented to reduce the risks these vulnerabilities may pose.The scope of this document will follow 3 main assets which require attention as they contain a lot of risk that could be mitigated. The users of this document will be Alan Hake(CEO), Amanda Wilson (CIO), Paul Alexander (CISO), William Freud (Mrg. Systems), and Scotty Doohan (Mrg. Applications).

2. Risk Assessment and Risk Treatment Methodology:

○ 2.1 Risk Assessment:

1. The process:

To be able to properly categorize the assets of DHAEI and assess the risks, we require a step by step process to follow, for when DHAEI require not only this risk assessment but any risk assessment..

First we need to gather any information required of any changes or planned changes to DHAEI as well as a list of their requirements. This is where we would involve the CIO Amanda Wilson, to provide the information. As well that the HR consultant Melinda Hixon for personnel information.

Secondly, after obtaining the list of all of the current and planned changes/ assets, we can then begin to categorize them into a chart from most to least impact on the company if the assets were ever compromised.

Next, we assign the risks to the risk owners, which are associates that are in charge of the responsibility to make the decision of accepting the possible risk to the company or mitigating the risk.

Next, we provide possible mitigation/ treatment methods to any potential risks DHAEI may face and contact. This is where we would involve the proper managers or executives in charge of the risks to make their decisions on accepting or mitigating the risks. This is where we can involve people like the CIO Amanda Wilson, the CISO Paul Alexander, Mgr. of Sys. William Freud, and Mgr. of App. Scotty Doohan, for example.

Finally, The last plan of action is to implement the mitigation or treatment methods for the risks that have been provided.

2. Assets, vulnerabilities, and threats:

The 3 main assets are as follows:

1. DHAEI's ability to provide its internet services to its users.

2. DHAEI's privacy in the form of their user accounts.

3. DHAEI's company data.

Based on the information provided by DHAEI, there are 3 major risks that can be taken into account when moving ahead with the planned changes and current assets.

1. Where user data is stored during the data transfer.

2. Remote associates accessing the network through an unsecure connection.

3. Data loss from data transference to the new branch office.

These are 3 potential high impact risks that DHAEI currently face, the first one is having user data stored in the FSI. This poses a great risk to the company as there may be security concerns in relation to storing the user data for the new members on the FSI database, then if it is compromised or accessed by an unauthorized user, then the private user data can be manipulated to breach any info desired by an attacker. The second major risk is the remote users only using an L2TP (Layer 2 Tunneling Protocol) VPN (Virtual Private Network) connection to access the network. Usually when using a VPN that condenses data into a packet, an encryption service is needed so that the data can be transferred securely and not accessed during the transfer. Finally, data loss from data transferring from the main branch to the new branch. Data loss during a transfer is a normal occurrence, and not having the proper contingencies to recover the lost data will hinder the operations of the new branch.

3. Determining the risk owners:

When determining the risk owners we have to take into account who will not only be the owner of the risks we will identify the main owners of the risks as well as any contributors that could contribute to the assessment of the risks involved.

1.**User Data store on FSI**: The main owner of this risk would be Amanda Wilson (CIO), as they are the executive in charge of information operations. The contributors to this risk will be William Freud (Mrg. Systems) and their branch of associates, as they are in charge of system operations they will help the transfer of user data from the FSI to the new branch. As well as Paul Alexander (CISO) and his branch of associates as they are in charge of security operations, they will be in charge of securing the data and ensuring that there are no compromises to user data.

2.**Remote access through unsecure VPN**: The main owner of this risk would be William Freud (Mrg. Systems), and the contributors will be Paul Alexander (CISO) and his associates. William Freud being the manager of systems is incharge of the technological aspect of the network, and therefore would be helping the remote workers by providing them with the computers and VPN’s to make secure access to the network possible. With the help of Paul Alexander and his associates monitoring and providing the security for the remote workstations.

3. **Data loss on transfer**: The main owner of this risk would be William Freud(Mrg.Systems), the contributors would be the associates under William Freud, as well as Cecilia Thompson (Mrg. Networking) and the associates under them. William Freud will be responsible for the maintenance of the data being transferred and its validity. The contributors will be responsible for ensuring the process goes as smoothly as can be and that the information stays secure for the network.

4. Impact and likelihood:

Risk	Impact (0-10)	Likelihood (0-5)
User data on FSI	10	4
Unsecure Remote Access	10	3
Data loss on Transfer	4	4

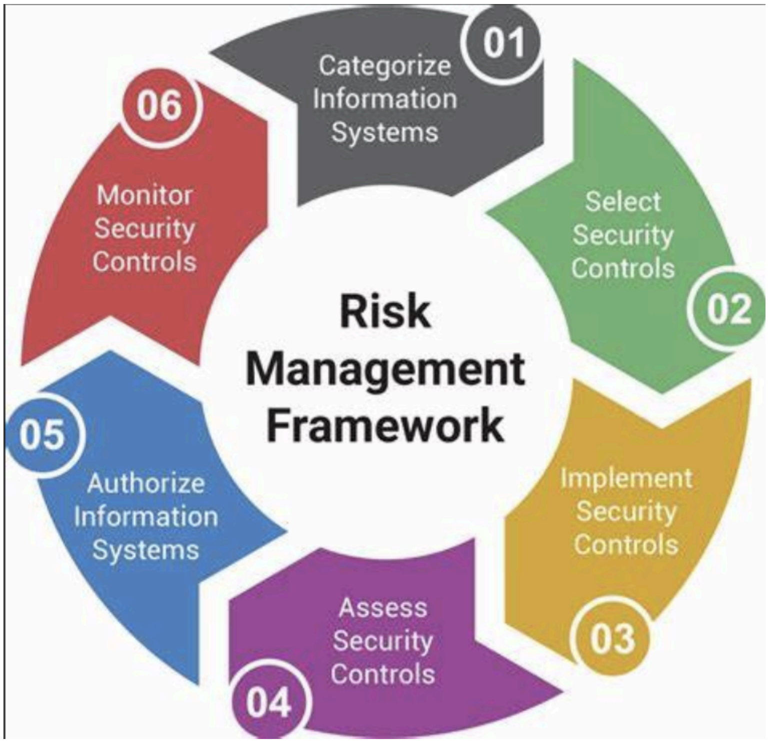
The impact scores as seen on the table above are determined by how much the risks could prevent workflow operations to the company if compromised. The user data being stored on the FSI until the data transfer is rated as a 10, as since this is dealing with user accounts for the new branch that is being secure in a database not meant to be as secured for user information, if accessed by an unauthorized user or an attacker with malicious intent, would compromise not only the user account data but would also grant administrative access to the network which could lead to several types of attacks such as Ransomeware. Ransomware is an attack where a malicious attacker steals and encrypts a company's data and extorts the company for monetary gain. The likelihood of this happening is at just above moderate (4) because the likelihood of this vulnerability being exploited is not a guarantee but there is still a good possibility of the vulnerability being exploited.

5. Risk acceptance criteria:

The criteria that is needed to be met when accepting the risks involved are if the risk must have minimal or effective mitigation in order to accept the risk, the risk in question must also have someone to take responsibility if the worse case scenario happens. As stated above, the higher the risk that the company takes, the more impact it will have if compromised, but some risks can be ignored or treated to be a lower risk such as the data loss upon transfer. This risk has minimal impact to DHAEI because even though it hinders some operations there can be effective treatments in order to reduce the amount of risk or impact it would have. Taking precautions such as having back ups of data securely stored will ensure that any lost data can be recovered from the original database lowering the impact from a (4) to possibly a (2) for instance.

- ### 2.2 Risk Treatment:

Using the RMF (Risk Management Framework) standard procedure when categorizing and mitigating risks, we can minimize or even eradicate certain risks and their severity levels on the company. First is categorizing the risks as seen in section 2. We categorize the examples of 3 risks to the company that pose the more important vulnerabilities. The first one being User data being stored on FSI, second being Unsecure remote access to the network, and lastly data loss on transferring to the new branch. Categorizing them on their impact and likelihood, as well as the importance to the company will determine how prioritized they will be. After categorizing we follow the rest of the steps of the RMF as follows:


Risk Management Framework
01
Categorize Information Systems
02
Select Security Controls
03
Implement Security Controls
04
Assess Security Controls
05
Authorize Information Systems
06
Monitor Security Controls

1. Categorize
2. Select Security Controls
3. Implement Controls
4. Assess Controls
5. Authorize Systems
6. Monitor Controls

The proposed treatment methods or Security Controls are as follows:

To mitigate the potential risk of malicious attackers or unauthorized associates managing to view the data on the FSI, there are a few standard operating procedures (SOP) to help mitigate this risk. One of the most effective being “Principle of Least Privilege”, this SOP makes sure that only certain users have permissions to read or edit certain files on a system, this will ensure that only authorized associates can view or edit the new user data being stored.

The next risk we will propose a treatment for is the unsecure remote access from the remote associates. Initially having a vpn does help with a layer of security when access the network, but since the condensed files do not have any protection and are readable to anyone with access to them, it becomes a risk to the company as anyone can hijack the data to insert malicious code, or any other means of infiltrating the network as well. To mitigate this risk we would need to ensure that the data being accessed or sent remotely is encrypted to make the information less accessible to onlookers not with the company. Programs such as IPSec (Internet Protocol Security) will provide the encryption service for the L2TP (Layer 2 Tunneling Protocol) VPN. This will lessen the risk to the company and treat the current problem at hand.

The last risk we will be looking at is the data loss when transferring data to the new branch. The SOP (Standard Operating Procedure) for this risk is to ensure there are back ups of the data before sending files over. Running a full diagnostic as to what information is being transferred to the new branch and having a copy made in case of file corruption is the first part of the SOP when confronting this risk, the next part of the SOP is to run another diagnostic of the files after they have been transferred, to see if any data has been corrupted or lost, then making a list of what has been lost to make a request to send those files in particular again so all the information can be restored. Following the SOP for all 3 of these risks will significantly reduce the risk involved when categorizing each risk to DHAEI.

Work Cited

Mocan, T. (2021, March 1). *What is L2TP (layer 2 tunneling protocol)?*. CactusVPN. https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-l2tp/

Computer Security Division, I. T. L. (n.d.-a). *About the RMF - NIST risk management framework: CSRC*. CSRC. https://csrc.nist.gov/Projects/risk-management/about-rmf

What is the principle of least privilege?. Palo Alto Networks. (n.d.). https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege

Oyaro, J. (2023, April 22). *IPSec VPN: What it is and how it works*. Privacy Affairs. https://www.privacyaffairs.com/ipsec-vpn/