RISK MANAGEMENT PLAN

Fahad Shahzad

P5

Purpose, Scope, and Users

The purpose of this document is to define the methodology for assessment and treatment of information risks in MHS, and to define the acceptable level of risk according to the NIST 800-53 standard. Risk Assessment and Risk Treatment will be applied to the entire scope of the ISMS (i.e., to all assets which are used within the organization, or which could have an impact on information security within the ISMS).

The Users of this document are all employees of DHAEI, who take part in Risk Assessment and Risk Treatment.

Note: all data is classified as confidential.

Risk Assessment and Risk Treatment Methodology:

Risk Assessment:

The process:

Risk Assessment is implemented through the Risk Assessment Table. The Risk Assessment process is coordinated by the information security analyst, identification of threats and vulnerabilities is performed by asset owners, and assessment of consequences and likelihood is performed by risk owners. DHAEI in selective situations will have the same asset owner and risk owner for a given asset.

Furthermore, the individuals/groups that will partake (according to the given data) will be the Security, Systems, and the Network teams with the respective managers and techs, and more importantly the CIO and the COO.

The Security Team, more importantly those reporting to Paul Alexander (CISO) are responsible for handling matters related to security, documentation, and raising potential risk while ensuring security measures.

The Systems Team, or rather more specifically those reporting to William Freund (Mgr. Systems) in particular, the system and network administrators. These are the individuals who are responsible for the organization's computer activities, data processing, along with network and data security.

The Network Team, more importantly the individuals that are reporting to Cecilia Thompson (Mgr. Networking), whose responsibilities are to ensure that the network resources are made available to all users in an efficient manner and as quickly as possible.

Assets, vulnerabilities, and threats:

The requirements set the DHAEI are the following:

1. Technical Requirements
    - DHAEI must meet the following technical requirements:
    - Ensure that all company-issued computers receive all updates that have been approved for release by the technology department.
    - Minimize Internet bandwidth by providing internal computers with Microsoft updates via internal servers.
    - Minimize traffic across the VPN for remote users.
    - Provide central monitoring of all servers.
    - Generate an email whenever a hardware event occurs on any of the servers in the company.
    - The support technicians located in the branch office must have the rights to perform all local maintenance on the branch office servers in their respective branches.
    - The installation of the new RODC in the Brampton office must minimize active directory replication across the WAN link between Columbus and the main office storage space to store user data must be minimized.
    - All company-issued computers must be configured with Office 365.
2. Security Requirements
    - DHAEI must meet the following security requirements:
    - The branch office technicians should not have any rights to servers not located in their respective branch offices.
    - The installation of the new RODC in the Brampton office must not require any passwords or cached secrets to be stored outside of company servers.
    - Files stored on the company file servers must be protected in the event that a file server or the drives from any file server are stolen.
3. User Requirements
    - DHAEI must meet the following user requirements:
    - Users in the new branch office must access their data using mapped drives.
    - User drives should not need to be remapped when the data is moved from the main office file server to the branch office server.

The Assets they have outlined are listed below:

- Windows server 2019

- Windows 10 stations
- 2 Domain controllers
- One File server
- One Windows software update service.
- One infrastructure server

After reviewing the requirements set out by the DHAEI, the following are the possible vulnerabilities or threats found:

The first main threat is the temporary setup of the data storage of the new users from the Brampton, Mississauga branches. Where their data is stored on the FSI (File server) and there by allows the user to use the mapped drives to access that very data. The vulnerability being giving new users can access by extension to the entire File Server.

The second threat is the lack of security on remote connections for users connecting to the main network. Although users are using the L2TP VPN, however the organization hasn't implemented any way to enhance security of the remote connections (ie. MFA).

The third vulnerability are the people and their lack of awareness about security standards or potential social engineering threats. This opens the organization to a lot of vulnerabilities and other threats such as phishing or code injection attacks.

Determining the risk owners:

After reviewing the vulnerabilities and threats above along with the other resource is mentioned by the DHAEI organization the following are the risk owners for each of the following threats and vulnerabilities:

For the first threat and vulnerability which spoke of the data storage risk in relationship to the file server the risk owners will be the network team and the system team. The network team due to making sure that all users are aware of how to back up their data and how to re map their drives and the new processes that will be implemented whereas a system team will make sure That all organizations computer activities network and security processes or forwarded to the individuals in question. The respective managers will curate the report and implement the changes before emailing the reviewed report too the CIO and COO.

The second threat and vulnerability which spoke of the remote connection and the lack there of security between the users and the network itself using the L2TP VPN. The risk owners will be the security team and the system team. The security team will take charge of implementing and designing of the security measures such as for example MFA, while the system team will take charge of making sure the network changes are recorded and implemented effectively for all the users who will be using remote services. The respective managers will then curate and implement the changes before emailing they reviewed report to the CIO and the COO.

Finally, the 3rd and final threaten vulnerability that we have discussed or the people. The risk owners that will be involved will be all three teams. The security team will create the documentation and the processes to follow, the system will capture all computer activities that occur from the user end, and the network team will make sure that all the information is provided to the end user in an effective and timely manner. The respective managers will then curate and implement the changes before emailing the reviewed the report to the CIO and COO.

Impact and likelihood:

After risk owners have been identified, it is necessary to assess impacts for each combination of threats and vulnerabilities for an individual asset if such a risk materializes:

High Impact	**7-10**	Loss of confidentiality, availability, or integrity has considerable and/or immediate impact on the organization's cash flow, operations, legal or contractual obligations, or its reputation.
Mid Impact	**4-6**	Loss of confidentiality, availability, or integrity incurs costs and has a low or moderate impact on legal or contractual obligations, or the organization's reputation.
Low Impact	**0-3**	Loss of confidentiality, availability, or integrity does not affect the organization's cash flow, legal or contractual obligations, or its reputation.

After the assessment of consequences, it is necessary to assess the likelihood of occurrence of such a risk.

High Likelihood	**4-5**	Existing security controls are low or ineffective. Such incidents have a high likelihood of occurring in the future.
Mid Likelihood	**2-3**	Existing security controls are moderate and have mostly provided an adequate level of protection. New incidents are possible, but not highly likely.
Low Likelihood	**0-1**	Existing security controls are strong and have so far provided an adequate level of protection. No new incidents are expected in the future

Threat	Vulnerability	C	I	A	Overall Risk
User access to File server					9:4
	Data Leak	10:5	8:4	4:2	
	Code injection	10:5	10:5	6:2	
	Corruption of data	10:5	10:5	10:5	
VPN access					8:4
	Account Hijacking	6:2	8:4	5:3	
	Malware installation	9:3	10:3	10:5	
People					9:4
	Social engineering	6:3	10:5	8:4	

Risk acceptance criteria:

After reviewing the criteria and the threats mentioned above in the table along with the requirements outlined by the organization it has come to our knowledge that the most imperative threats to keep an eye on will be the file server access to the average user and the storage of data along with the education and awareness building for everyday users.

Risk Treatment:

First off, the risk that presents a threat to the file servers, a potential action plan to mitigate the threat or vulnerability is as follows:

- Do not allow users to store data on the file servers but rather they should store the data locally on the workstation themselves.
- The data that is stored locally should then be backed up using backup applications such as Avamar or cloud applications like Google Drive.
- Once the read only domain controller has been installed, we can then download and push the backup files to the domain controller itself.
- This method allows for no direct interaction from the user two of the file server thus protecting the data.

Secondly, the risk that presents a threat to the remote connection and the users working remotely, a potential action plan to mitigate the threat or vulnerability is as follows:

- have the 20 users that work remotely install a multi factor authenticator for example Microsoft authenticator or RSA.
- with the multifactor authenticator generating random tokens this method adds on an extra layer of security to the VPN which is better than the static passwords that the programmers we're using beforehand

Finally, the risk that presents a threat and manipulates the people to gain access to the organizations data and network hey potential action plan to mitigate the threat of an ability is as follows:

- document all security procedures and measures and simplify it for the average non-technical individual.
- provide training and guides of how to look out for potential threats and vulnerabilities.
- implement processes or tools which allow users to report potential threats and bone abilities.
- restrict and manage access to users appropriately using groups and policies as needed.

Executive Summary

The DHAEI organization comprises of numerous assets and network controllers such as windows servers, windows clients, domain controllers, file servers call my DNS network service and Windows Update services. There are about 1500 users, 200 users are in branches and 20 users work from home remotely using a VPN connection.

We have been informed that the organization will be opening two new branches in Brampton and Mississauga respectively. We have been informed that the branches will store user data on the file servers until the read only domain controllers can be installed and the data migrated.

After reviewing the technical, security and user requirements presented by the organization, we have discovered 3 distinct threats and vulnerabilities. These include access issues related to data storage on the file servers and user accessing that very central file server, Remote VPN access not being secure, and lastly the lack of processes and documentation provided to users on how to detect security risks and how to avoid them at a user level.

For these threats and vulnerabilities starting with de file storage, we have decided to implement cloud storage or backing up data to the local device, then migrating the data over once the read only domain controller is installed. Implementing multi factor authentication for added security to remote VPN connections. Finally documenting and educating using training programs to inform users how to detect and report potential threats and vulnerabilities.

During the documentation, implementation and monitoring of these threats and vulnerabilities we will be working with the risk owners who are the respective managers and department heads who will curate reports for the CIO and the COO for each step of the process.

References

Welcome to Compass. (n.d.). https://web.compass.lighthouselabs.ca/p/13/projects/risk-management#eval-rubric

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). *About the RMF - NIST Risk Management Framework | CSRC | CSRC*. https://csrc.nist.gov/projects/risk-management/about-rmf

CVE - Search CVE list. (n.d.). https://cve.mitre.org/cve/search_cve_list.html