Project 5: Risk Management Case Study

By Evelyn Wolfe

Executive Summary

DHAEI has contracted our team to review the current infrastructure, and develop a comprehensive risk assessment focused for the opening of the new office in Brampton Mississauga. This assessment identifies critical threats, evaluating their potential impact on the Confidentiality, Integrity, and Availability of the information assets and outlines recommended mitigation strategies following the ISO 27001 standards. Our primary objective is to ensure that the Information Security Management Systems (ISMS) at this new location both supports DHAEI's operational requirements and fulfills legal and regulatory obligations.

In conducting our review, we focused on the physical office environment, core IT Infrastructure -including server, and network devices-and the end-users desktops, credential policies. Although DHAEI has multiple offices and remote users across Ontario Canada, this assessment specifically targets the new office at Brampton Mississauga, but with consideration for the broader, company-wide security framework.

We centered our analysis on three main threats: End-User Computing - Impersonation, Server Malfunction - Hardware Failures, and Building Physical Security - Unauthorized Access. With respect to End-User Computing - Impersonation reviews weak or lost credentials and the likelihood of unauthorized access, and we recommend controls to enforce strong passwords, multi-factor authentication(MFA,) and rigorous security awareness training. Regarding the potential of server malfunction and the failure of the hardware, our concern lies with operation disruption, possible data loss, and unplanned downtime. We advise implementing regular maintenance schedules, on and off site data backup, and robust disaster recovery incident response procedures. Finally addressing Building Physical Security - Unauthorized Access and the impact of gaps in the security measures that the building may be exposed to. Our recommendations in mitigating the issues of unauthorized entry goes over using controlled access systems (ie: key cards, and biometrics) CCTV Monitoring, visitor logs with facility escorting, and employee training on tailgating - a situation where an unauthorized individual follows an authorized employee into a secure area.

Throughout this risk assessment, we adhered to the ISO 27001 standards and its relevant annex With respect to the following annex controls: Access Management (A.9,) Physical Security (A.11,) Backup and Recovery (A.12, and A.17,) as well as security incident handling (A.16.) By integrating these best business practices, DHAEI reinforces its commitment to maintaining a robust compliant ISMS at the new office.

Risk Management Plan

Our goal is to create a comprehensive risk assessment for the new location at Brampton Mississauga. This will detail a comprehensive risk assessment for the location, including treatment methodologies to address current security issues and establish a strategy for monitoring potential future risk and vulnerabilities.

Purpose, Scope, and Users

Purpose:

The purpose of this risk assessment is to assess and mitigate potential risk for DHAEI's new location Brampton Mississauga. This will include the implementation of a threat methodology to addressing current issues and establishing a monitoring strategy for potential future vulnerabilities. At the end of this risk assessment, there will be a clearly defined goal that ensures that the Information Security Management Systems (ISMS) align with DHAEI specific needs, risks, and legal obligations as outlined in the ISO 27001 Framework.

Scope:

The scope of this assessment is focused on the new office location in Brampton Mississauga and support for approximately two hundred employees within this specific location. The assessment will define the boundaries of the ISMS, clearly identify the assets, processes and systems that will be included. This scope will address the information security needs within this specific office, with consideration to the local and remote access security, network infrastructure, and data protection. DHAEI values data redundancy; therefore, all data created at the Brampton Mississauga location is backed up at the Oshawa Headquarters. While the risk assessment is tailored to the Brampton Mississauga location, it is within the consideration and aligns with the risk management framework of the headquarters as much as possible.

Users:

This risk assessment specifically targets the two hundred employees at the Brampton Mississauga location. The scope of the users-related responsibilities includes defining roles, implementing appropriate access controls, and ensuring that all employees receive the necessary training on information security policies and procedures. Although DHAEI is a large company that has multiple offices in Ontario, and many remote users, this framework is focused on the new office treatment located in Brampton Mississauga, and the support for around two hundred employees. This is specifically tailored to the two hundred employees.

Risk Assessment and Risk Treatment Methodology

Risk Assessment

The Process:

In this document, we will be reviewing the process of the items within the scope and how they impact the Information Security Management System (ISMS.)

In order to establish the scope and the context, a review of the current system needed to be analyzed to determine the resolution at the Brampton Mississauga location. We defined the following as the scope; End User Computing, Server, Networking, and Building Physical Security. End User Computing is the devices for the employees within this location, this would include laptops, desktops and any other users devices. Server is the local Read Only Domain Controller that also acts as a File Server. Networking is defined as the routers, switches and the firewall. Finally the Building Physical Security is detailed as the entry points, locks, and the security access system. Our goal is to prevent the breach of our confidentiality, integrity, and availability of these items.

Assets, Vulnerabilities and Threats:

WIth an organization like DHAEI, there is multiple items that would be important to protect from vulnerabilities and threats. As ISO 27001 defines that we identify the assets, their vulnerabilities and threats.

End User Computing

End User Computing is defined as the Users Assets such as Laptops, Desktops and other devices that would hold data. There are multiple vulnerabilities, but our focus is on weak passwords, outdated software, lost or stolen devices and privilege abuse or misuse. A threat actor could take advantage of these vulnerabilities through malware, phishing, impersonation, theft of device, or even an insider threat.

For example a vulnerability that would impact one of these devices: CVE-2024-43491 is detailed of an issue Microsoft has identified with in Windows 10 update in August of 2024, that caused vulnerabilities that were previous patched out a earlier date in 2015 to become an issue again after this August 2024 update. However Microsoft did make the remedy with September 2024 patches, there was a brief period that the equipment was left to these vulnerabilities.
CVE website. (n.d.-d). https://www.cve.org/CVERecord?id=CVE-2024-43491
NVD - cve-2024-43491. (n.d.). https://nvd.nist.gov/vuln/detail/cve-2024-43491

Server

The Server Asset is specifically identified as the Read Only Domain Controller that also acts as a File server at the new Brampton Mississauga location. We have assigned the following vulnerabilities; misconfiguration in the settings, weak credentials, inadequate patching and

updates, privilege abuse. The major threats that could be taken advantage of would be data breaches, unauthorized access, server malfunctions, malware that targets the server.

To support these claims, CVE-2024-6769 has been identified as an attacker that would target a server via a DLL Hijacking through remapping of a drive with a poisoning impact on the cache. This would impact Windows Server 2015, Windows Server 2019, and Windows Server 2022, as well as end user devices that run Windows 10, and Windows 11. The research into this threat is still early, and originally reported on September 26 2024, with no recent updates.
CVE website. (n.d.). https://www.cve.org/CVERecord?id=CVE-2024-6769
NVD - cve-2024-6769. (n.d.). https://nvd.nist.gov/vuln/detail/cve-2024-6769

Networking

We have identified the assets associated with the Networking Category as the routers, switches, firewalls, access points and VPN gateways. These vulnerabilities are defined as using the default configuration, lack of encryption, insufficient monitoring, physical tampering. Regarding the threats, a well known threat against the network would be Denial of Service or DOS, as well as eavesdropping, unauthorized configuration changes, and router compromise.

To support the threat and vulnerabilities, a known vulnerability within CISCO Software for the Cisco Ultra-Reliable Wireless Backhaul (URWB) Access Point that would allow a remote, unauthorized attacker to access the system via an injection attack with root privileges on the operating system. This type of vulnerability has been identified through improper validation of input to the web-based management interface for these access points. The attacker would then be able to send HTTP requests to the web-based management interface on the targeted system, with success of the exploit, the attack then would have root privileges to the targeted device.
CVE website. (n.d.-c). https://www.cve.org/CVERecord?id=CVE-2024-20418
NVD - CVE-2024-20418. (n.d.). https://nvd.nist.gov/vuln/detail/CVE-2024-20418

Building Physical Security

The last bullet point in the review of DHAEI Brampton Mississauga office is the Physical Security of the building. Even though physical security is not in the realm of the Information Security Management System (ISMS,) the breach of physical security can lead to other compromises that would impact the other assets above. We identify the physical security as the following: entry points (doors and/or gates,) locks, badge systems, surveillance cameras. Some vulnerabilities are unsecured entry points, lack of monitoring, outdated systems that support badge systems or surveillance cameras, as well as outdated access control mechanisms. The threats that would be associated with these vulnerabilities may look like unauthorized access, theft of end user equipment or other items, sabotage of the facility, and other environmental risk such as fires, or flooding.

Although there is no recorded CVE, there are impacts that physical security breaches could impact any CVE. Most important, physical security has an impact on risk mitigation by

identifying the vulnerabilities and prioritizing what would be critical first. This helps maintain the other industry standards before they become indicators of compromise.
Technology, T. L. E. (2024, March 1)
https://www.securityindustry.org/2024/03/01/navigating-the-security-landscape-a-quick-guide-to-cve-for-young-professionals/

DHAEI RISK Assessment

Organizational Unit: Brampton/Mississauga New Branch Office

		Risk Assessment								
ID #	Function	Asset Name	Asset Owner(s)	Threat	Vulnerability	Impact (0-2)	Likelihood (0-2)	Risk (=I+L)	ISO27001 CONTROL REFERENCE	Risk owner
1	End User Computing	Desktops and Laptops	Help Desk - Tina Witherly and Carlos Mendez							Julian Vasque Help Desk Manager
		Context: Company provided work desktops, and laptops used for employee productivities								
				Theft / Lost	Facility Breech	0	0	0	A.11.1.3	
				Impersonation	Weak password /weak PIN/ Lost ID	1	1	2	A.9.3.1	
					Privilege abuse	1	1	2	A.9.2.6	
				Malfunction	Hardware Failure	0	1	1	A.7.13	
				Malicious Software	Malware, Virus,	2	1	3	A.12.2.1	
2	Server	BramptonFS	Systems Administrators							William Freund Systems Manager
		Context: A server that provides read-only access to the domain controller and stores local files critical for business operations.								
				Theft / Lost	Facility Breech	0	0	0	A.11.2.9	
				Imsersonation	Privilege abuse	1	1	2	A.9.2.6	
					Weak Admin Credentials	2	1	3	A.9.2.6	
					Loss Id/credential	0	1	1	A.9.3.1	
				Malfunction	Hardware Failure	2	1	3	A.7.13	
				Malicious Software	Malware, Ransomware	2	1	3	A.12.2.1	
3	Network Infrastructure	Routers	Network Administrators							Cecilia Thompson Networking Manager
		Context: Devices enabling network inbound traffic, segmentation, and connectivity.								
				Theft	Unauthorized Access	2	1	3	A.9.1.2	
				Network Distruption	Misconfiguerd Routing Tables	2	1	3	A.5.29, A.12.4.3	
				Malicious Traffic	Lack of Firewall Rules	2	1	3	A.13.1.1.	
				Malfunction	Aging Hardware	2	1	3	A.9.1.2	
4	Building Security	Building Entry Points	Corporation Security - Robert Briscoe Facility Operations - TBD							Paul Alexander - CISO Chief Infomration Security Officer
		Context: Crucial part of controlling the physical security access to the facility and ensuring only authorized users have access								
				Theft	Theft of Equipment	2	1	3	A.11.1.2	
				Tailgating	Lack of Enforcement via Badge	1	2	3	A.11.1.5	
				Fire or Flood Damage	Lack of Environmental Controls	2	1	3	A.11.2.2	
				Unauthorized Access	Compromised Building Procedures	2	1	3	A.11.1.3	

Source of Table provided by Lighthouse Labs: LHL Risk Assessment Table

The Risk Owners

Through the research, we have broken down the Assets to associated risk owners.An indepth overview projection for Brampton Mississauga new office may look like the following:

- **Risk Owner for Unauthorized Access Physical Access**
    - Facilities Manager: TBD
        - Ensures physical controls are in place
        - Conducts periodic audits regarding the entry points
    - Chief Information Security Officer: Paul Alexander
        - Implements the security monitoring systems and badge systems
        - Coordinate with facilities to address and identify vulnerabilities
    - Chief Information Officer: Amanda Wilson
        - Sets policies and budgets for physicals and logical security
        - Review risk reports and approves mitigation

  Reference: ISO 27001 Appendix A.11.1.1, A.11.1.2, A.11.1.4

- **Risk Owner for Impersonation (Weak Password/Weak PIN/Lost UID) End User Computing**
    - Help Desk Technician: Tina Witherly and Carlos Mendez
        - Providing password resets supports and meet the security policies
        - Reporting Lost ID or UID and disabling compromised accounts
    - IT Security Technician: Harold Fry
        - Enforcing strong authentication requirements (MFA, Password Complexity Rules)
        - Monitoring and reporting suspicious login attempts
    - Chief Information Security Officer: Paul Alexander
        - Defining the enterprise password standards and requirements
        - Overseeing audits of users credentials and access logs
        - Ensuring training programs are implemented and are tied to lost credentials and weak passwords

  Reference: ISO 27001 Appendix A.5.1.1, A.9.2.1, A.9.4.2

- **Risk Owners for Malfunction Hardware on Server**
    - Manager of Systems: William Freund
        - Monitoring Server Health
        - Maintaining and reporting on hardware replacement plans and review of backups
    - Chief Information Security Officer: Paul Alexander
        - Implementing the redundancies that DHAEI has implement to maintain high-availability
        - Overseeing and Coordinating disaster recovery plan for hardware failure
    - Chief Information Officer: Amanda Wilson

- Maintaining the budget and allocating funds for server hardware refreshes and updates/upgrades
- Ensuring the goals between the server reliabilities and DHAEI objectives are aligned

Reference: ISO 27001 Appendix: A.11.1.4, A..12.3.1, A.12.5.1, A.17.2.1, A.18.1.5

Impact and Likelihood

Impact and Likelihood Table: Physical Security Risks						
Threat/Risk	Impact on (C/I/A)	Confidentiality (0-10)	Integrity (0-10)	Availability (0-10)	Likelihood (0-5)**	Notes
Unauthorized Building Entry	C/I	8	6	5	3	Unmonitored entry could expose sensitive documents and allow tampering with secured systems.
End User Computing - Impersonation (Weak Passwords/Weak PIN/Lost UID	C/I	7	5	4	4	Compromised credentials could lead to unauthorized system access, exposing sensitive data or disrupting operations.
Server - Malfunction (Hardware Failure)	A	4	3	8	2	Hardware failure could disrupt critical services, impacting business continuity and data availability.

Risk Acceptance Criteria

The Highest Risk Item - End User Computing - Impersonation (Weak Passwords/Weak PIN/Lost UID)

Likelihood: 4

Based on the table examples above, the highest risk item for the new location - Brampton Mississauga is the End User Computing - Impersonation (Weak Passwords/Weak PIN/Lost UID.) We marked **Confidentiality** at a 7 of 10, this is due to users' credentials being compromised and sensitive data would be released to the public from a threat actor. **Integrity** is rated at a 5 out of 10 due to unauthorized access that may lead to leak or deletion of critical data at DHAEI, this could also cause other issues with the accuracy of records. We recorded the **Availability** at a 4 out of 10 due to the potential risk that disruption of services or systems may be locked out for other employees from the downtime of malicious actions.

The Minimized Risk Item - Server - Malfunction (Hardware Failure)

Likelihood: 2

This has been classified as a lower-risk item, due to the potential failure of physical hardware. While hardware malfunctions are relatively rare to begin with, the impact on the C/I/A varies due to the factors from the redundancy, encryption, and backup procedures that DHAEI strives for. **Confidentiality** was rated a 4 out of 10, as hardware failure could result in mishandling or improper disposal of physical components, potentially exposing the sensitive data. **Integrity** is rated 3 out of 10, this is due to the rarity of hardware malfunction and that these failures do directly cause corruption of the data integrity. With the current scope of redundancy and data back up, DHAEI would make data recoverable. Finally the **Availability** is rated a 8 out of 10, this is due to the impact at the Brampton Mississauga location, and the delays while the fail overs kick in to the Headquarters. With the current setup of the RODC server, there is a redundancy setup, and the major issue would be the File Server that is local at this new site.

Risk Treatment and Methodology

End User Computing - Impersonation (Weak Passwords/Weak Pin/Lost UID)

Based on the threat or vulnerability that we have identified above with weak authentication methods risk the chances of being impersonated. These users could also suffer from lost or stolen credentials and even impersonation when the attacker might contact the help desk under false pretenses to gain unauthorized access.

In order to mitigate these types of breaches, DHAEI has incorporated a couple of policies and education plans for the end users. On DHAEI side, we can incorporate strong policies regarding the complexity of passwords, using Multi Factor Authentication, as well as training. Furthering our team monitoring team in the Security Operation Center monitoring for account lockouts and multiple failed login attempts in a short period of time. For the End User, constant education regarding security awareness is important to be completed in a timely manner. We also run regular phishing simulation, commonly simulated via a tool like KnowBe4.

ISMS Online (2023, December 14) *ISO 27001 – Annex A.9: Access Control*. https://www.isms.online/iso-27001/annex-a-9-access-control/

Server - Malfunction (Hardware Failure)

We Identified critical issues associated with potential server hardware failure, although we ranked this item lower in the likelihood and risk acceptance, there is still a means to have a plan in place for the outages and disruptions this may cause.

In order to provide the best options for mitigation, we will want to focus on maintenance, redundancy, and disaster recovery testing and plans. By offering redundancy and a failover solution, we prevent the interruptions associated with the down time. It is important that DHAEI maintains their back ups onsite and offsite, and has a disaster recovery site setup for the critical infrastructure. Furthering the preventative maintenance of the server, we prevent these issues from occurring. Finally having an incident response setup and a disaster recovery plan in the works and that has been fine tuned and tested will help with any issues whether it is a system failure or the disaster of flood or fire.

ISO 27001 Annex A.11: Physical and Environmental Security | HiComply. (n.d.). https://www.hicomply.com/hub/iso-27001-annex-a-11-physical-and-environmental-security
A.11.2 - Equipment

Building Physical Security - Unauthorized Access

After reviewing the risk assessment regarding the physical location of the new office at Brampton Mississauga, we strive to make sure that the physical security is detailed within the assessment to prevent any unauthorized access. If the location lacks these physical security

measures, then a threat actor could breach the facility and gain access to sensitive equipment, data, or other assets. This could result in both a cyber and physical compromise.

While there may be many different options in mitigation, we strongly recommend the following: controlled access systems, surveillance and monitoring systems, and employee security awareness. In order to access any facility or prevent unauthorized users access, key cards or biometrics would help. This would also prevent employees from other branches from accessing an unapproved branch they have not been cleared for yet. Also maintaining an entry log from visitors, with physical escorts would be important. Having a detailed surveillance and monitoring system like CCTV setup, would allow real-time monitoring and prevention of suspicious behavior from happening. Finally, the education of the employees is also a key factor in this defensive strategy, this would provide the employees with knowledge on tailgating prevention, badge procedures and protocols, and what to do if an unknown visitor is walking around without an escort.

ISO 27001 Annex A.11: Physical and Environmental Security | HiComply. (n.d.). https://www.hicomply.com/hub/iso-27001-annex-a-11-physical-and-environmental-security
A.11.1.1, A.11.1.1

Statement of Applicability (SoA)

While essential to ISO 27001 compliance, this document provides an overview of Annex A controls for DHAEI identified risk, including those that are excluded. Each risk identified during the assessment process has been mapped to specific controls, particularly Appendix A controls like A.9 - Access Control, and A.11 - Physical Security. With each identified control, DHAEI has documented the current implementation, detailing the purpose and how it is enforced with any policies or procedures. Non-applicable controls are clearly marked and accompanied by a rationale for exclusion. We attempt to keep the transparency of DHAEI risk treatment strategy and maintenance alignment to ISO 27001 requirements.

Citations and References

Kosutic, D. (n.d.). *ISO 27001 Risk Assessment & Risk Treatment: The Complete guide*. Advisera

https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/

Annex Controls References:

ISMS. Online (2023, March 28). ISO 27001:2022 Annex A 7.13 - Equipment Maintenance. https://www.isms.online/iso-27001/annex-a/7-13-equipment-maintenance-2022/

Inverifi. (2023, May 10). ISO 27001 Controls - Annex A.9: Access control https://inverifi.com/iso-27001-annex-controls-overview/iso27001-controls-annex-a-9-access-control/

HiComply (2023, July 25). ISO 27001 Annex A.11: Physical and Environmental Security https://www.hicomply.com/hub/iso-27001-annex-a-11-physical-and-environmental-security

ISMS. Online (2023, December 14). ISO 27001 – Annex A.12: Operations Security. https://www.isms.online/iso-27001/annex-a-12-operations-security/

HiComply (2023, July 25). ISO 27001 Annex A.16: Information Security Incident https://www.hicomply.com/hub/iso-27001-annex-a-16-information-security-incident-management