LIGHTHOUSE LAB

CYBERSECURITY

RISK MANAGEMENT CASE STUDY

DHA ENTERPRISE INC

DANIEL O. OLUWAYALE

Content Page

Executive Summary

The idea of Risk Assessment and Management is rooted in the idea that a business can't control its fate. To mitigate this risk, a company needs to be able to identify which risks are most important, and how it can best manage them. Lighthouse Labs. (n.d.). DHAEI is a growing software development company with multiple offices and remote workers. As the company expands, the risk of data breaches, system downtimes, and hardware failures increases, making it essential to have a robust Risk Management Plan in place. This plan provides a comprehensive approach to identifying, assessing, and mitigating risks across the company's network infrastructure, server environment, and user systems.

Key risks identified include cybersecurity threats, hardware failures, and data loss/unauthorized access. Cybersecurity threats are the most pressing risk due to the increasing use of remote work and cloud services. Mitigation measures for cybersecurity risks include enhanced endpoint security, employee training, and strong network defenses. Hardware failures, while less likely, still pose a risk to business continuity and will be addressed through redundancy and improved monitoring. Data loss and unauthorized access are also critical risks, particularly with mobile devices and branch offices, and will be mitigated through encryption, access control, and regular backups.

This Risk Management Plan serves as a guide for DHAEI to address these risks systematically and ensure the company’s infrastructure and data remain secure as it continues to grow. The plan also provides a clear chain of responsibility for managing these risks from ground-level technicians to executive management.

Purpose

A business may face different types of risks, such as financial risk, strategic risk, security risk, etc. Therefore, it needs a risk assessment and management process to identify these risks and find ways to remediate them in a timely manner. Lighthouse Labs. (n.d.).

The purpose of this Risk Management Plan is to identify, assess, and manage risks that could potentially impact on the operational continuity, data security, and infrastructure reliability of DHAEI. The plan will outline the steps and processes for identifying and mitigating risks and will serve as a guide for making informed decisions about risk treatment.

Scope

The scope of this plan covers the entire DHAEI network infrastructure, including its main office in Oshawa, branch offices, remote workers, and planned expansion in Brampton,

Mississauga. The plan includes the company's network infrastructure, server environment, user systems, and security protocols.

Users

1. Amanda Wilson, CIO – Superintends DHAEI's information and risk management program.
2. Paul Alexander, CISO – Manages the security risks and treatments.
3. IT Support Technicians – Implement security control and ensure the optimal operation of the infrastructure.
4. Security Team – Contribute to risk assessments, treatments and monitoring processes

Risk Assessment and Risk Treatment Methodology

2.0 Risk Assessment

2.1 The Process: This risk assessment plan is prosecuted on the risk assessment table. Potential risks across the infrastructure are first identified and analyzed by asset owners and the assessment of the repercussion and likelihood is performed by risk owners i.e. Amanda, Paul and other Tech Managers

2.2 Assets, Vulnerabilities, and Threats

The primary threats DHAEI may face are:

- **Cybersecurity threats like hacking, malware attacks, and data breaches** – With DHAEI's reliance on cloud services and remote workers, cyberattacks could compromise sensitive data.
    - *Challenges*: Vulnerabilities in user devices, remote access connections (L2TP VPN), and cloud platforms (Rackspace and AWS). Improper Authentication (CWE-287); when an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct. MITRE Corporation. (n.d.)
- **Hardware failure or system downtime** – Failure of critical infrastructure, such as file servers or domain controllers, could cause significant downtime, impacting all users.
    - *Challenges*: Lack of redundancy in branch office infrastructure and insufficient hardware monitoring. CWE-400 – Uncontrolled Resources Consumption; Limited resources include memory, file system storage, database connection pool entries, and CPU. If an attacker can trigger the allocation of these limited resources, but the number or size of the

resources is not controlled, then the attacker could cause a denial of service that consumes all available resources. MITRE Corporation. (n.d.).

- **Data loss and unauthorized access** – The potential for data loss or unauthorized access due to physical theft (e.g., of file servers or laptops) or improper security configuration.
    - *Challenges*: CWE (326) Inadequate encryption strength; a weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current attack methods and resources. MITRE Corporation. (n.d.) Inadequate encryption and access controls, with branch offices and most especially remote workers

2.3 Determining the risk owner

For each risk, a risk owner has to be identified—the person or organizational unit responsible for each risk. This person may or may not be the same as the asset owner. Lighthouse Labs. (n.d.).

- Cybersecurity Threats – Ground level; security technicians who carry out the security configuration to the Mid-Level; Paul Alexander that oversees security controls and ensure everything is secure to the Executive Level; CIO, Amanda manages security risks and aligns the management with company goals.
- Hardware Failures – IT support technicians that address tech issues and monitor servers to Paul that manages system monitoring, to Amanda that oversees all the process.
- Data Loss and unauthorized – From the IT support technicians that implement encryption and backup measures to Paul who manages or monitors security practices related to securing data and to Amanda who ensures risk mitigation are enforced.

1.4 Impact and Likelihood

Risk/Threat	Impact (CIA)	Impact Score (0-10)	Likelihood	Likelihood Score (0-5)
Cybersecurity Threats	Confidentiality Integrity	8	Likely	4
Hardware Failure	Availability	7	Unlikely	2
Data Loss/Unauthorized Access	Confidentiality Integrity, Availability	9	Possible	4

- Cybersecurity Threats have a high impact on confidentiality and integrity, with a high likelihood of occurrence because of remote access to the developers and cloud services.
- Hardware Failure is less likely to happen compared to the other threats, but the impact would be high if the hardware systems are unavailable.
- Data Loss/Unauthorized Access has the highest impact on confidentiality, integrity, and availability and it is somewhat likely due to vulnerabilities in remote offices.

1.5 Risk Acceptance Criteria

- Most Likely/Highest Risk is the Data loss/Unauthorized Access and should be prioritized as its occurrence would to a great extent disrupt the operation of the organization as data loss will result to the unavailability of data if not backed up. By manipulating stored data, adversaries may attempt to affect a business process, organizational understanding, and decision making. MITRE Corporation. (n.d.).
- Ignored/Minimized Risks is hardware failure can be ignored temporarily as it's less likely to happen or can be easily corrected by initiating proper monitoring systems.

2.0 Risk Treatment

2.1 Cybersecurity Threats:

- Mitigation: Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials but be aware of Authentication. Interception techniques for

some two-factor authentication implementations. Multi-Factor. MITRE Corporation. (n.d.). Strengthen network security with robust firewalls, use of MFA for remote access and train employees extensively to reduce phishing attacks.

- Priority: High – due to the potential damage to data and the high likelihood of attack.

2.2 Hardware Failure:

- Mitigation: Retain cold-standby or replacement hardware of similar models to ensure continued operations of critical functions if the primary system is compromised or unavailable. MITRE Corporation. (n.d.). Implement redundancy for key infrastructure, enhance server monitoring systems, and ensure regular maintenance schedules are in place.
- Priority: Medium – because it is unlikely but could lead to significant downtime if not addressed.

2.3 Data Loss/Unauthorized Access:

- Mitigation: Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise. Maintain and exercise incident response plans [1], including the management of gold-copy back-up images and configurations for key systems to enable quick recovery and response from adversarial activities that impact control, view, or availability. MITRE Corporation. (n.d.). Use full disk encryption on all company laptops, implement strict access controls, and ensure file server encryption. Regular backups and offsite storage for disaster recovery should be established.
- Priority: High – due to the impact on confidentiality and integrity, especially in the event of theft.

Reference

Lighthouse Labs. (n.d.). *NIST Risk Management Framework*. *Compass*. https://web.compass.lighthouselabs.ca/p/cyber/days/w04d4/activities/2980

Lighthouse Labs. (n.d.). Intro to Cyber Security Risk Assessment.*Compass*.https://web.compass.lighthouselabs.ca/p/cyber/days/w04d4/activities/2979

MITRE Corporation. (n.d.). *CWE-326: Inadequate Encryption Strength*. Common Weakness Enumeration. https://cwe.mitre.org/data/definitions/326.html

MITRE Corporation. (n.d.). *CWE-400: Uncontrolled Resource Consumption*. Common Weakness Enumeration. https://cwe.mitre.org/data/definitions/400.html

Lighthouse Labs. (n.d.). *Sample risk management plan* [PDF]. Lighthouse Labs. https://learningimages.lighthouselabs.ca/Cyber+BC/Cyber+BC+C5/Cyber+BC+C5.2/Sample+Risk+Management+Plan.pdf

MITRE Corporation. (n.d.). *TA0040: Impact*. MITRE ATT&CK. https://attack.mitre.org/tactics/TA0040/

MITRE Corporation. (n.d.). *T1133: External Remote Services*. MITRE ATT&CK. https://attack.mitre.org/techniques/T1133/

MITRE Corporation. (n.d.). *M0811: Secure Network Engineering*. MITRE ATT&CK. https://attack.mitre.org/mitigations/M0811/

MITRE Corporation. (n.d.). *M0953: Application Layer Protocols*. MITRE ATT&CK. https://attack.mitre.org/mitigations/M0953/