Risk Management Plan

DHA Enterprise Inc. (DHAEI)

Table of Contents

1. Executive Summary

This Risk Management Plan for DHA Enterprise Inc. (DHAEI) outlines a systematic approach to identifying, assessing, and treating the cybersecurity risks faced by the company. DHAEI is a software development company, and given the sensitivity of its data and remote infrastructure, it is imperative to prioritize cybersecurity. The plan has been developed in accordance with the **ISO 27001 Risk Management Framework** (ISO, n.d.), utilizing resources like the **NIST National Vulnerability Database (NVD)** (NVD, n.d.) and the **MITRE ATT&CK Framework** (MITRE ATT&CK®, n.d.) for vulnerability identification.

Key risks include **data breaches**, **ransomware attacks**, and **insider threats**. The mitigation strategies focus on implementing **multi-factor authentication (MFA)**, enforcing a **comprehensive patch management program**, and enhancing **access control mechanisms**. These strategies ensure that DHAEI meets its technical, security, and user requirements, safeguarding the organization's critical assets.

2. Introduction

2.1 Purpose

The purpose of this Risk Management Plan is to systematically identify, evaluate, and address risks to DHAEI's information security framework by implementing the ISO 27001 Risk Management Framework (ISO, n.d.). This plan aims to provide a structured approach for mitigating risks, safeguarding sensitive assets, and ensuring business continuity amid the growing threats in the software development landscape.

2.2 Scope

This Risk Management Plan encompasses the entire digital infrastructure of DHAEI, which includes its main office in Oshawa, Ontario, branch offices, remote working environments, data storage systems, and core software development processes. The scope involves identifying and assessing risks related to the confidentiality, integrity, and availability of critical business assets (CIA triad) within the organization. Special attention is given to the interaction between internal staff, including the Chief Information Officer (CIO) Amanda Wilson, Chief Information Security Officer (CISO) Paul Alexander, and their respective teams, to ensure that risk management practices align with DHAEI's operational goals (ISO, 2013).

2.3 Users

This document is intended for DHAEI's executive management, including CEO Alan Hake, CIO Amanda Wilson, and CISO Paul Alexander, along with the IT and security teams responsible for executing the company's cybersecurity initiatives. It also serves as a guide for external stakeholders such as security auditors and managed service providers (MSPs), ensuring that all parties involved understand their roles in maintaining and enhancing DHAEI's cybersecurity posture.

3. Risk Assessment and Risk Treatment Methodology

3.1 Risk Assessment

3.1.1 Process

The risk assessment process for DHAEI follows the structured approach outlined in the ISO 27001 framework, ensuring a thorough understanding of the organization's security landscape. This process consists of:

1. **Identifying Critical Assets:**
   This includes the organization's data servers, development environments, sensitive client information, and remote access VPN systems that facilitate work for employees, particularly the 20 programmers working from home.
2. **Assessing Vulnerabilities:**
   This step involves identifying potential weaknesses in systems that could be exploited. For example, outdated software on internal workstations may expose DHAEI to vulnerabilities documented in the Common Vulnerabilities and Exposures (CVE) list (CVE-2018-17890 | NVD, n.d.). Additionally, insufficient access controls, such as weak passwords or lack of account lockout policies, can be points of exploitation (CVE-2023-34240 | NVD, n.d.).
3. **Determining Threats:**
   Evaluating potential external and internal threats is essential for maintaining the integrity of DHAEI's operations. For instance, data breaches can occur from external threat actors using phishing tactics, as described in MITRE's ATT&CK framework, which identifies common techniques such as Spear Phishing that can lead to credential theft and unauthorized access (T1566 | MITRE ATT&CK®, n.d.).
4. **Assigning Risk Ownership:**
   Key personnel across various levels of the organization, from IT technicians managing system security to executive management, are involved in the risk assessment process to ensure comprehensive oversight and accountability.

3.1.2 Assets, Vulnerabilities, and Threats

The critical assets identified for DHAEI include:

- **Data Servers:**
  These servers store sensitive client data and intellectual property (IP), making them a prime target for cyber threats. NIST Special Publication 800-53 (NIST, 2020) outlines the necessity for strong access controls and encryption for protecting data at rest and in transit.
- **Remote Access Infrastructure (VPN):**
  Used by employees for secure access, the VPN can be a vulnerability if not configured correctly. Implementing NIST's recommendations on secure remote access can help mitigate risks associated with this infrastructure, including the use of VPNs configured to utilize robust encryption methods and multi-factor authentication.
- **Internal Workstations:**
  Employee workstations are susceptible to insider threats, as highlighted in the Government of Canada guideline (Canada, 2024), which encourages organizations to monitor user activities and implement measures to detect anomalous behavior.

3.1.3 Determining the Risk Owners

For each identified risk, a clear chain of responsibility is established, ensuring accountability from technical staff to senior management:

- **Technicians (Branch Office):**
  Responsible for implementing day-to-day security measures, including patching and monitoring systems. They utilize tools like the Security Content Automation Protocol (SCAP) to automate vulnerability management and compliance.
- **Paul Alexander (CISO):**
  Oversees all security operations at DHAEI, ensuring that risks are communicated to executive management and mitigated appropriately. Paul implements risk management strategies aligned with the NIST Risk Management Framework (RMF), focusing on continuous monitoring and assessment.
- **Amanda Wilson (CIO):**
  Ensures that all technological systems remain current and compliant with established security protocols, facilitating smooth operations across all offices. She relies on NIST's guidance for integrating risk management into the organization's strategic planning.
- **Alan Hake (CEO):**
  Provides oversight and strategic direction for risk management, ultimately responsible for ensuring the organization's overall security posture. The CEO should endorse the risk management framework outlined in NIST SP 800-39 (NIST, 2011) which emphasizes the importance of integrating risk management into enterprise governance.

3.1.4 Impact and Likelihood

The table below outlines the three primary threats to DHAEI, detailing their potential impact on confidentiality (C), integrity (I), and availability (A), as well as their likelihood of occurrence, along with the assigned risk owner.

Threat	CIA Affected	Impact (0-10)	Likelihood (0-5)	Risk Owner
Data Breaches	Confidentiality	9	4	Paul Alexander (CISO)
Ransomware Attack	Availability	8	3	Amanda Wilson (CIO)
Insider Threats	Integrity	6	2	Branch Office Technicians

3.1.5 Risk Acceptance Criteria

DHAEI will prioritize high-impact risks, such as data breaches and ransomware attacks, which necessitate immediate mitigation efforts, as per the guidance in ISO 27001. Lower-impact risks, like insider threats, may be addressed based on resource availability. Risks will be accepted based on their likelihood of occurrence and the cost-effectiveness of the proposed mitigation measures.

3.2 Risk Treatment

The treatment strategies for the identified risks at DHAEI are as follows:

1. **Data Breaches**:
   Implement Multi-Factor Authentication (MFA) for all remote access, secure VPN tunnels, and enhance encryption protocols for sensitive data to comply with NIST's guidelines for protecting sensitive information (NIST, 2017)

- **Priority**: High (immediate implementation)

2. **Ransomware Attacks**:
   Strengthen the patch management process by ensuring all software is current, and implement regular data backups to minimize downtime and data loss. These strategies align with MITRE's recommendations for proactive defense against ransomware (T1486 | MITRE ATT&CK®, n.d.).
   - **Priority**: Medium (important but not as immediate as MFA)
3. **Insider Threats**:
   Establish enhanced user access controls to restrict employee privileges and actively monitor for suspicious activities within the network. This strategy follows NIST's guidance on managing insider threats (CSF Tools, 2023).
   - **Priority**: Low (due to lower likelihood but remains a necessary measure)

Risk Treatment Table

Risk Type	Treatment	Residual Risk	Responsible Owner
Data Breaches	MFA, secure VPN, enhanced encryption	Low	Paul Alexander (CISO)
Ransomware Attack	Patch management, regular backups	Medium	Amanda Wilson (CIO)
Insider Threats	User access control, active monitoring	Low	Branch Office Technicians

4. Statement of Applicability (SOA)

The following ISO 27001 controls have been applied to mitigate the identified risks:

- **A.9 Access Control**: Multi-factor authentication (MFA) has been implemented to secure remote access and reduce the likelihood of unauthorized access, mitigating the risk of data breaches (G, 2023).
- **A.12.3 Backup**: Regular, automated data backups are performed to ensure business continuity in the event of a ransomware attack, allowing for quick recovery without significant data loss (Dange, 2024).
- **A.9.2 User Access Management**: Enhanced user access controls and monitoring policies are in place to restrict user privileges, minimizing the risk of insider threats and preventing unauthorized changes (G, 2023).

5. Technical, Security, and User Requirements

This Risk Management Plan takes into consideration DHAEI's:

- **Technical Requirements**: Including secure VPN access, multi-factor authentication, and regular system patching to maintain the integrity and availability of critical

systems. These measures help prevent data breaches and ensure network reliability for remote employees.

- **Security Requirements**: Aligned with the ISO 27001 framework, these requirements focus on safeguarding the confidentiality, integrity, and availability (CIA) of DHAEI's critical systems, addressing specific threats such as data breaches, ransomware, and insider risks.
- **User Requirements**: Ensuring that remote employees and in-office staff can access necessary systems securely while maintaining efficiency and minimizing disruptions to daily operations.

6. Conclusion

This Risk Management Plan provides a clear and actionable roadmap for DHAEI to address key cybersecurity risks, including data breaches, ransomware attacks, and insider threats. By adhering to the ISO 27001 framework and implementing the recommended risk treatment strategies, DHAEI can significantly reduce its exposure to these risks while maintaining operational continuity. Furthermore, ongoing risk assessments and continuous monitoring, as outlined in the NIST Risk Management Framework, will ensure that DHAEI adapts to emerging threats and remains resilient in an evolving cybersecurity landscape.

7. References

1. Canada, C. S. E. (2024, June 4). How to protect your organization from insider threats (ITSAP.10.003). Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/how-protect-your-organization-insider-threats-itsap10003-0
2. CSF Tools. (2023, December 23). Access control management - CSF tools. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/critical-security-controls/version-8/csc-6/
3. Dange, P. (2024, May 22). ISO 27001: 2022 - Control 8.13 information backup. https://iso-docs.com/blogs/iso-27001-2022-standard/iso-27001-2022-control-8-13-information-backup
4. G, M. (2023, December 27). ISO 27001 - Annex A.9 - Access control. https://iso-docs.com/blogs/iso-27001-standard/iso-27001-annex-a-9-access-control
5. ISO/IEC 27001:2022. (n.d.). ISO. https://www.iso.org/standard/27001
6. National Institute of Standard and Technology (2020, September). NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for information systems and organizations. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
7. National Institute of Standard and Technology (2011, March). NIST Special Publication 800-39 Managing Information Security Risk. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf
8. MITRE ATT&CK®. (n.d.). https://attack.mitre.org/
9. National Institute of Standards and Technology (2017, June). Digital Identity Guidelines. NIST Special Publication 800-63-3. https://pages.nist.gov/800-63-3/sp800-63-3.html
10. NVD - Vulnerabilities. (n.d.). National Vulnerability Database. https://nvd.nist.gov/vuln