Risk Management Plan for DHA Enterprise Inc. (DHAEI)

Table of Contents

INTRODUCTION **1**

PURPOSE, SCOPE, USERS **1**

ROLES AND RESPONSIBILITIES **1**

1. RISK ASSESSMENT AND RISK TREATMENT METHODOLOGY **2**

1.a. Risk assessment: process 2
1.b. Assets, vulnerabilities, and threats 2
1.c. Determining the risk owners 3
1.d. Impact and likelihood 4
1.e. Risk Acceptance Criteria 4

2. RISK TREATMENT **5**

3. EXECUTIVE SUMMARY **6**

REFERENCES **7**

Introduction:

The Risk Management Plan for DHA Enterprise Inc. (DHAEI) serves as a comprehensive guide to identify, assess, and mitigate risks associated with its information systems and assets. This document outlines the purpose, scope, users, risk assessment methodology, risk treatment strategies, and executive summary.

Purpose:

The purpose of the Risk Management Plan is to provide DHAEI with a structured approach to identifying, assessing, and mitigating risks related to its information systems and assets. By clearly defining the purpose, DHAEI ensures that all stakeholders understand the objectives of the plan and can work towards achieving them effectively.

Scope:

The scope of the Risk Management Plan outlines the boundaries and extent to which the plan applies. This includes all aspects of DHAEI's operations, including its main office, branch offices, remote work environments, network infrastructure, servers, software, and data. By defining the scope, DHAEI ensures that no critical areas are overlooked in the risk management process.

Users:

The users of the Risk Management Plan are the individuals or groups responsible for implementing and overseeing risk management activities within DHAEI. This includes senior executives, department heads, risk management professionals, and other relevant stakeholders. By identifying the users, DHAEI ensures that the plan is tailored to the needs and responsibilities of its intended audience. The primary users of this plan include DHAEI's management team, comprising CEO Alan Hake, CIO Amanda Wilson, Chief Information Security Officer Paul Alexander, and other department heads responsible for operational functions.

Roles and Responsibilities:

Senior Management:

Role: Senior management, including CEO Alan Hake and CIO Amanda Wilson, provides overall leadership and direction for the risk management process.

Responsibilities: Approve the Risk Management Plan and associated policies. Allocate resources and support for risk management activities. Review and endorse risk treatment strategies and decisions. Monitor the effectiveness of risk management efforts and ensure compliance with organizational objectives.

Risk Management Team:

Role: The risk management team, led by the Chief Information Security Officer (CISO) Paul Alexander, is responsible for executing the risk management process and implementing risk treatment strategies.

Responsibilities: Identify, assess, and prioritize risks to DHAEI's information systems and assets. Develop risk treatment plans and recommend appropriate controls and measures. Implement and monitor risk mitigation efforts, including controls implementation and performance monitoring. Report regularly to senior management on risk status, trends, and effectiveness of risk treatments.

Department Heads:

Role: Department heads, such as heads of IT, operations, and finance, are responsible for managing risks within their respective departments.

Responsibilities: Identify department-specific risks and vulnerabilities. Implement controls and measures to mitigate identified risks. Ensure compliance with risk management policies and procedures. Report significant risks and incidents to the risk management team and senior management.

Employees:

Role: All employees, including technical staff, support staff, and management, play a crucial role in identifying and managing risks within their areas of responsibility.

Responsibilities: Identify and report potential risks, vulnerabilities, and security incidents. Adhere to organizational policies and procedures related to risk management and information security. Participate in training and awareness programs to enhance understanding of risks and mitigation measures. Collaborate with the risk management team to implement and maintain effective controls and measures.

1. Risk Assessment and Risk Treatment Methodology:

The risk assessment methodology describes the approach and techniques used to identify, analyze, and evaluate risks. This may include methods such as risk workshops, interviews, surveys, and risk matrices. By defining the risk assessment methodology, DHAEI ensures consistency and accuracy in assessing risks across the organization. The risk treatment strategies outline the actions and measures taken to mitigate or manage identified risks. This may include implementing controls, transferring risks through insurance, accepting risks within tolerance levels, or avoiding risks altogether. By documenting risk treatment strategies, DHAEI ensures that appropriate actions are taken to address identified risks effectively.

1.a. Risk Assessment: Process:

- The risk assessment process involves a systematic approach of identifying threats, vulnerabilities, and potential impacts.
- Stakeholder engagement includes Alan Hake, Amanda Wilson, Paul Alexander, department heads, and frontline staff.

1.b. Assets, Vulnerabilities, and Threats:

- Key threats identified include data breaches, system outages, and unauthorized access.
- Challenges include maintaining security amidst rapid expansion and managing access control across multiple locations.

Below is the classification table of Asset Names and Asset Owner with the possible threats and vulnerabilities.

Asset Name	Asset Owner	Threat	Vulnerability
Network Infrastructure	The Chief Information Officer(CIO)	DOS Attacks targeting network devices such as Routers and switches.	Weak network segmentation allowing unauthorised access to critical network resources.
Servers	The Chief Information Officer(CIO)	Malware Infections Targeting server operating systems or applications.	Outdated server software with known security vulnerabilities.
Software Applications	The Chief Information Officer(CIO)	Application Layer attacks, such as SQL injection or cross site scripting targeting web applications.	Lack of input validation leading to exploitable code injection vulnerabilities.
Data (Customer Information, Intellectual Property)	The Chief Information Security Officer(CISO)	Data breaches resulting in unauthorised access, disclosure, or theft of sensitive information.	Inadequate data encryption or access controls, allowing unauthorised users to view or modify sensitive data.
Active Directory Domain	The Chief Information Security Officer(CISO)	Credential Theft or brute force attacks targeting Active Directory credentials.	Weak or default passwords, inadequate access controls, or misconfigured group policies.
File Server	The Chief Information Security Officer(CISO)	Ransomware Attacks encrypting files stored on the server for extortion.	Lack of regular data backups, allowing ransomware to cause permanent data loss.
Workstations (Desktop, Computers)	The Chief Information Officer(CIO)	Social engineering attacks, such as phishing emails, targeting employes to gain unauthorised access.	Unpatched operating systems or software, leaving workstations susceptible to known exploits.
Remote Access Infrastructure(VPN)	The Chief Information Security Officer(CISO)	MitM attacks, intercepting VPN connections to steal credentials or inject malicious code.	Weak encryption protocols or insecure VPN client configurations.

Cloud Infrastructure (AWS)	The Chief Information Officer(CIO)	Cloud Service misconfigurations leading to unauthorised access or data exposure.	Inadequate identity and access management policies, allowing permissions for unauthorised users.

1.c. Determining the Risk Owners:

- The ownership of risks is established from frontline staff to senior executives, ensuring accountability and effective risk management at all levels.

Risk: Data Breach

Ground Level Owner: IT Security Analyst
Responsibilities:

- Monitor network and system logs for suspicious activities.
- Implement security controls to prevent unauthorized access.

Middle Level Owner: Chief Information Security Officer (CISO)
Responsibilities:

- Oversee the IT security team and incident response procedures.
- Review and analyze security reports and incident investigations.

Senior Executive Level Owner: Chief Information Officer (CIO)
Responsibilities:

- Set the strategic direction for information security initiatives.
- Allocate resources for security investments and risk mitigation efforts.

Risk: Malware Infection

Ground Level Owner: System Administrator
Responsibilities:

- Install and update antivirus software on all systems.
- Monitor systems for signs of malware activity and perform regular scans.

Middle Level Owner: IT Manager
Responsibilities:

- Develop and enforce policies for software usage and system maintenance.
- Coordinate with the security team to ensure timely response to malware incidents.

Senior Executive Level Owner: Chief Technology Officer (CTO)
Responsibilities:

- Evaluate and select cybersecurity solutions to enhance malware detection and prevention.
- Provide guidance on IT infrastructure design and architecture to minimize malware risk.

Risk: Insider Threat (Unauthorized Access)

Ground Level Owner: Human Resources Manager
Responsibilities:

- Conduct background checks and employee screening during the hiring process.
- Educate employees on security policies and acceptable use of company resources.

Middle Level Owner: Chief Human Resources Officer (CHRO)
Responsibilities:

- Develop and enforce policies for access control and employee monitoring.
- Collaborate with IT and security teams to identify and address insider threat risks.

Senior Executive Level Owner: Chief Executive Officer (CEO)
Responsibilities:

- Set the tone for a culture of security awareness and accountability throughout the organization.
- Review and approve high-level policies and procedures related to insider threat mitigation.

1.d. Impact and Likelihood:

- A detailed table presents the impact and likelihood of identified threats, facilitating a structured understanding of potential risks and their severity.

Threat/Risk	Impact on C, I, A	Extent (0-10)	Likelihood (0-5)
Data Breach	**C**: 9, **I**: 8, **A**: 7	8	4
Malware Infection	**C**: 7, **I**: 6, **A**: 8	7	3
Insider Threat (Unauthorized access)	**C**: 8, **I**: 7, **A**: 6	7	2

Data Breach:

Impact on C (Confidentiality): 9 - A data breach can expose sensitive customer information and intellectual property, resulting in severe reputational damage and legal liabilities.
Impact on I (Integrity): 8 - A data breach may result in the modification or corruption of data, leading to loss of trust and credibility in the integrity of DHAEI's systems and operations.
Impact on A (Availability): 7 - A data breach may disrupt operations, leading to downtime or loss of access to critical systems and services.
Likelihood: 4 - Data breaches are relatively common in today's threat landscape, with attackers constantly probing for vulnerabilities to exploit.

Malware Infection:

Impact on C (Confidentiality): 7 - Malware infections may result in unauthorized access to confidential data, leading to potential data leakage or theft.
Impact on I (Integrity): 6 - Malware can tamper with or modify files and system configurations, compromising the integrity of DHAEI's data and systems.
Impact on A (Availability): 8 - Malware infections can disrupt operations by causing system crashes, network outages, or loss of access to critical resources.
Likelihood: 3 - Malware infections are common and can occur through various attack vectors, such as malicious email attachments or compromised websites.

Insider Threat (Unauthorized Access):

Impact on C (Confidentiality): 8 - Insider threats can result in the unauthorized access or disclosure of sensitive information to unauthorized parties.
Impact on I (Integrity): 7 - Insider threats may involve intentional or accidental manipulation or alteration of data, compromising its integrity.
Impact on A (Availability): 6 - Insider threats may disrupt operations by intentionally or inadvertently deleting or altering critical files or system configurations.
Likelihood: 2 - While insider threats are a concern, they are less common than external threats and may require insider access or knowledge to execute.

1.e. Risk Acceptance Criteria:

Impact of Most Likely / Highest Risk Item (e.g., Data Breach): The most likely or highest risk item, such as a data breach, could have severe consequences for DHAEI, including:

Financial Loss: Legal fines, forensic investigations, and potential lawsuits could lead to significant financial losses.
Reputational Damage: Loss of customer trust and confidence could damage DHAEI's reputation and hinder business opportunities.
Operational Disruption: Business operations may be disrupted, affecting productivity and service delivery.
Regulatory Non-Compliance: Failure to comply with data protection regulations could result in legal penalties and damage to DHAEI's regulatory standing.

Reasons for Ignoring or Minimizing Other Items: Some items in the risk table may be ignored or minimized for the following reasons:

Low Impact or Likelihood: Risks with low potential impact or likelihood may not warrant significant resources for mitigation.
Resource Constraints: DHAEI may lack the resources or expertise to address certain risks effectively.
Existing Controls: Risks may be adequately mitigated through existing controls or measures, reducing the need for additional intervention.
Strategic Considerations: DHAEI may strategically choose to accept or tolerate certain risks to maintain agility in a competitive market.

2. Risk treatment:

Here is a summary of the three main threats identified (data breach, malware infection, and insider threat), along with recommended mitigations and their prioritization.

2.a. Data Breach: A data breach could lead to unauthorized access or disclosure of sensitive information, resulting in financial losses, reputational damage, and regulatory non-compliance.

Recommended Mitigations:

- **Implement encryption:** Encrypt sensitive data both in transit and at rest to protect against unauthorized access.
- **Enhance access controls:** Implement access controls and least privilege principles to restrict access to sensitive data. Utilize multi-factor authentication (MFA) to enhance authentication security.
- **Regular audits and monitoring:** Conduct regular audits of user access logs and network activity to detect and respond to unauthorized access attempts promptly. Implement intrusion detection and prevention systems (IDPS) to monitor network traffic for suspicious activities.

Priority: High.

Explanation: Data breaches pose a significant risk to DHAEI's reputation, finances, and compliance status. Mitigating this risk should be a top priority to prevent severe consequences and align with industry best practices and regulatory requirements.

2.b. Malware Infection: Malware infections can compromise systems, disrupt operations, and lead to data loss or theft, resulting in financial losses and reputational damage.

Recommended Mitigations:

- **Endpoint protection:** Deploy advanced antivirus software with real-time scanning and behavior-based detection to prevent malware infections. Utilize endpoint detection and response (EDR) solutions for enhanced threat detection and response capabilities.
- **Security patches and updates:** Implement a robust patch management process to ensure timely deployment of security patches and updates for operating systems, applications, and firmware.
- **User awareness training:** Provide regular cybersecurity awareness training to employees to educate them about common malware threats, phishing attacks, and safe browsing practices.

Priority: Medium.

Explanation: While malware infections can have serious consequences, the likelihood of occurrence may be lower compared to other threats. Mitigating this risk is still important but may not require immediate allocation of resources as data breach prevention.

2.c. Insider Threats (UnauthorisedAccess): Insider threats, such as unauthorized access by employees or contractors, can result in data breaches, fraud, or sabotage, impacting DHAEI's operations and reputation.

Recommended Mitigations:

- **Access controls:** Implement granular access controls based on job roles and responsibilities to restrict access to sensitive data and systems. Regularly review and update access permissions as needed.
- **Employee monitoring:** Deploy user activity monitoring solutions to track and analyze user behavior, detecting suspicious activities indicative of insider threats. Ensure compliance with privacy regulations and obtain employee consent where required.
- **Incident response plan:** Develop and regularly test an incident response plan to effectively respond to and mitigate insider threat incidents. Clearly define roles and responsibilities, escalation procedures, and communication channels.

Priority: High.

Explanation: Insider threats can be challenging to detect and mitigate, making them a high priority for risk management. Implementing preventive measures and incident response capabilities aligns with industry best practices.

3. Executive Summary:

DHA Enterprise Inc. (DHAEI) operates as a software development company, providing essential internet services and hosting solutions to small office/home office (SOHO) individuals and organizations. As DHAEI continues to expand its operations and digital footprint, the importance of effective risk management becomes paramount to safeguarding its assets, reputation, and operations.

In light of this, a comprehensive Risk Management Plan has been developed to identify, assess, and mitigate risks associated with DHAEI's information systems and assets. Through a systematic risk assessment process, several key threats have been identified, including data breaches, malware infections, and insider threats. These risks pose significant challenges to DHAEI's operations, finances, and regulatory compliance.

To address these risks effectively, several recommendations for risk treatment have been proposed:

Data Breach Mitigation:

- Implement encryption measures following industry standards such as NIST SP 800-53 to protect sensitive data in transit and at rest.
- Enhance access controls and monitoring systems to detect and respond to unauthorized access attempts promptly.
- Develop incident response plans and conduct regular audits to ensure readiness and resilience in the event of a data breach.

Malware Infection Prevention:

- Deploy advanced antivirus solutions and endpoint protection mechanisms in accordance with industry best practices and frameworks.
- Establish robust patch management processes to ensure timely deployment of security updates and patches for operating systems and applications.
- Provide ongoing cybersecurity awareness training to educate employees about malware threats and safe computing practices.

Insider Threat Management:

- Implement role-based access controls (RBAC) and user activity monitoring solutions to prevent and detect unauthorized access by insiders.
- Develop clear policies and procedures for employee onboarding, offboarding, and access management to mitigate insider threat risks.
- Establish incident response protocols and channels for reporting and investigating insider threat incidents.

By prioritizing these risk treatment strategies and aligning them with industry standards and best practices, DHAEI can strengthen its cybersecurity posture, mitigate potential risks, and safeguard its operations and assets. It is imperative for DHAEI's leadership team to allocate resources and support the implementation of these recommendations to effectively manage risks and ensure the long-term success and resilience of the organization.

In conclusion, proactive risk management is essential for DHAEI to navigate the evolving threat landscape and maintain trust and confidence among its customers, partners, and stakeholders. By embracing a culture of security awareness and continuous improvement, DHAEI can position itself as a trusted provider of internet services while effectively managing cybersecurity risks in today's digital age.

Conclusion:

In conclusion, proactive risk management is essential for DHAEI to navigate the evolving threat landscape and maintain trust and confidence among its customers, partners, and stakeholders. By embracing a culture of security awareness and continuous improvement, DHAEI can position itself as a trusted provider of internet services while effectively managing cybersecurity risks in today's digital age.

References:

How to perform a cybersecurity risk assessment in 5 steps- https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step

How ISO 27001: complete 10 step implementation guide - https://blog.softexpert.com/en/iso-27001-10-step-implementation-guide/

Calculate Risk Tolerance - https://lh5.googleusercontent.com/uXwtuSlYD6rR3KoA9wMj2Nz_Gqqsx-HDzw94a8ygCJqaEbT1313VEkLfHOADXMizJU73sGUYzyWFzvnZDIXeK6M1sFeW5xfz0FmJopoC1MIgiQ5Kuk89zbMBZ6uFRtc4Dc4QDrw_TkqD0vPTLg

OpenAI. (n.d.). ChatGPT . Retrieved from- https://openai.com/chatgpt

Risk Assessment: Likelihood & Impact - https://pratum.com/blog/443-risk-assessment-likelihood-impact

Why Assigning a Risk Owner is Important and How to Do It Right - https://strategicdecisionsolutions.com/risk-owner/

What is risk management, and why is it important? - https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/

What are the most effective ways to identify risks to information confidentiality?- https://www.linkedin.com/advice/1/what-most-effective-ways-identify-risks-information-q8jfe

Risk acceptance criteria - https://www.sciencedirect.com/topics/engineering/risk-acceptance-criterion#:~:text=Risk%20acceptance%20criterion%20defines%20the,to%20initiating%20the%20risk%20analysis
and
https://encyclopedia.pub/entry/16620

Data Breach Preparedness for Your Businesses — Lessons from ISO 27001 - https://medium.com/@soumyajit.ascentworld/data-breach-preparedness-for-your-businesses-lessons-from-iso-27001-95ef48ba01e9#:~:text=In%20conclusion%2C%20embracing%20ISO%2027001,customer%20trust%2C%20and%20regulatory%20compliance.

ISO 27001 Protection Against Malware Policy: Ultimate Guide - https://hightable.io/iso-27001-protection-against-malware-ultimate-guide/