DHAEI Risk Management Case

By: Mahad Mohamood

Introduction

DHA Enterprise Inc. (DHAEI), a dynamic software development company based in Oshawa, Ontario, faces various IT-related risks that can potentially disrupt its operations and compromise sensitive data.

Founded in June 2019 by CEO Alan Hake, DHAEI provides essential services such as internet access, web registration, and hosting solutions, which are critical to its approximately 1,700 users. This Risk Management Plan is crafted to identify, assess, and mitigate risks, ensuring the organization’s IT infrastructure remains robust and secure.

Risk management Plan and Statement of Applicability (SOA)

The Risk management Plan identifies specific actions and controls needed to mitigate the risks outlined in the risk assessment. The Statement of Applicability (SOA) then documents which of these controls are implemented, partially implemented, or not yet implemented, and provides details on their objectives, applicability, and status. Together, they ensure that risk management efforts are systematically applied, monitored, and aligned with organizational policies and ISO 27001 standards.

Risk management plan

1. Purpose, Scope, and Users

Purpose: To identify, assess, and manage risks associated with DHAEI’s IT systems and operations, ensuring that potential threats are mitigated and organizational objectives are met.

Scope: Includes all critical IT assets, including servers, network infrastructure, and remote work setups, across the main and branch offices.

Users: The plan will be used by DHAEI's IT and security teams, including the CIO, IT managers, and security personnel, to guide risk management efforts and ensure compliance with security policies.

2. Risk Assessment and Risk Treatment Methodology

2.1 Risk Assessment

2.1.1 The Process:

- List all critical assets and their functions.
- Determine weaknesses and potential threats to the assets.
- Evaluate the likelihood and impact of each threat on the assets.
- Assign responsibilities for managing each risk.
- Create a risk assessment table and risk treatment plan.

2.1.2 Individuals to Involve:

- IT Security Manager: To provide insights into technical vulnerabilities and security controls.
- Operations Manager: To assess operational impacts and resource requirements.
- CIO: For strategic oversight and alignment with organizational objectives.

2.1.3 Assets, Vulnerabilities and Threats:

Assets:

- Active Directory Domain (DHA.com): Essential for user authentication and authorization.
- File Server (FSI): Crucial for data storage and access.
- Infrastructure Servers:
  - Domain Controllers (DCI, DC2): Vital for domain management and authentication.
  - WSUS Server (WSUSI): Important for managing and distributing updates.

    - DNS Server (DHADNS): Key for network services.

- Branch Office Servers: Manage local infrastructure and data for branch offices.

- Remote Work Setup: Includes VPN connections and laptops for remote access.

- Central Monitoring System: Critical for monitoring server health and performance.

- Email Notification System: Important for alerting on hardware events.

Vulnerabilities and Threats:

- Data Breaches: Unauthorized access to sensitive information.

    - According to NIST, a breach "is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for other than authorized purpose."(NIST, Breach)

- Physical Theft: Theft of equipment or servers.

    - According to science direct, "physical theft in the context of computer science refers to the act of stealing physical devices or copies of data containing sensitive information, such as CD/DVDs, USB drives, laptops, or printed materials, from an organization's premises. It can occur due to weak physical security or the carelessness of employees."(ScienceDirect, n.d.).

- Insider Threats: Malicious or negligent actions by employees or trusted individuals.

    - According to CISA, “The Cybersecurity and Infrastructure Security Agency (CISA) defines insider threat as the threat that an insider will use their authorized access, intentionally or unintentionally, to do harm to the

> department’s mission, resources, personnel, facilities, information, equipment, networks, or systems. Insider threats manifest in various ways: violence, espionage, sabotage, theft, and cyber acts.”

2.1.4 Challenges:

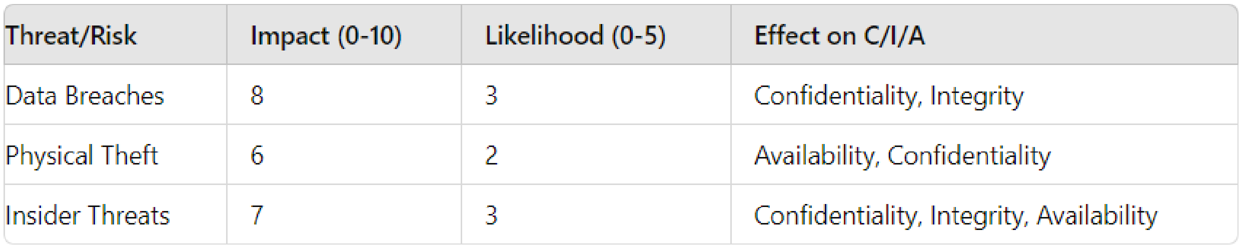
- Rapid Evolution of Threats: Keeping up-to-date with emerging threats.
- Resource Constraints: Limited budget and personnel for implementing security measures.
- Integration of New Systems: Ensuring new systems are secure and compliant.

2.1.5 Determining Risk Owners:

- Risk 1: Data Breaches
  - IT Security Manager: Manages data protection and access controls.
  - Compliance Officer: Ensures adherence to data protection regulations.
  - CIO: Oversees overall data security strategy.
- Risk 2: Physical Theft
  - Facilities Manager: Implements physical security measures.
  - IT Security Manager: Ensures equipment is securely stored.
  - CIO: Reviews physical security policies and resource allocation.
- Risk 3: Insider Threats
  - IT Security Manager: Monitors and enforces access controls.
  - Human Resources Manager: Conducts background checks and security training.

    - Operations Manager: Implements operational controls and ensures adherence.

Impact and Likelihood Table



Threat/Risk	Impact (0-10)	Likelihood (0-5)	Effect on C/I/A
Data Breaches	8	3	Confidentiality, Integrity
Physical Theft	6	2	Availability, Confidentiality
Insider Threats	7	3	Confidentiality, Integrity, Availability

2.2 Risk Treatment

2.2.1 Summary of Threats:

- Data Breaches: Moderate impact; affects confidentiality and integrity.

- Physical Theft: Lower likelihood; impacts availability and confidentiality.

- Insider Threats: Moderate impact; affects confidentiality, integrity, and availability.

2.2.2 Recommended Mitigations:

A . Data Breaches:

- Mitigations: Enhance data encryption, enforce strict access controls, and conduct regular security training.

- Priority: Medium, as it’s critical but less frequent.

- According to isms.online, "Data leakage is a frequent issue for organizations that manage large amounts of data, ranging from different classifications, on multiple distinct and interconnected IT systems, applications and file servers. ISO 27001:2022 Annex A 8.12 pertains to ICT operations which are conducted with system administrator access, and come under the umbrella of network management and maintenance."

B . Physical Theft:

- Mitigations: Strengthen physical security measures, use asset tracking systems, and implement secure storage practices.

- Priority: Low, given the lower likelihood but still important.

- According to isms.online, "ISO 27001:2022 Annex A 7.1 guarantees an organization can show it has suitable physical security boundaries in place to stop unauthorized physical access to information and other related assets."

C. Insider Threats:

- Mitigations: Implement strict access controls, conduct regular employee training, and perform thorough background checks.

- Priority: Medium, due to the potential for significant damage from trusted individuals.

- According to isms.online, "To comply with ISO 27001 Annex A control 5.7, organizations must do the following: Examine your threat environment periodically (by reviewing reports from government agencies and other organizations). Sources of threat (i.e., insiders, competitors, criminals, terrorist groups) should be identified. Determine possible novel attack vectors and trends based on current events and past incidents. The most important thing is to build defenses that will help mitigate security threats to the organization."

Statement of Applicability (SOA)

For each control, we will have a control object and specific measures outlined.

1. Access Control

Control Objective: Protect information by managing access.

- Control : A.9.1.1: Access Control Policy
- Measures: Establish and enforce policies for user access management.

- Control : A.9.2.3 Management of Privileged Access Rights
- Measures: Implement procedures for use of privileged access.

- Control : A.9.4.1: Information Access Restriction
- Measures: Restrict information access based on roles and responsibilities.

B. Cryptography

Control Objective: Protect data confidentiality and integrity through encryption.

- Control : A.10.1.1: Cryptographic Controls
- Measures: Use encryption for data at rest and in transit.

- Control : A.10.1.2: Key Management
- Measures: Manage encryption keys securely.

C. Physical and Environmental Security

Control Objective: Protect physical assets and infrastructure from threats.

- Control : A.11.1.1: Physical Security Perimeter
- Measures: Implement physical security measures for office and branch locations.

- Control : A.11.2.1 Equipment Siting & Protection
- Measures: Secure equipment with access controls and surveillance.

D. Operations Security

Control Objective: Ensure secure and effective operation of IT systems.

- Control : A.12.2.1 Controls Against Malware
- Measures: Implement malware controls and user awareness beyond just anti-virus software.

- Control : A.12.4.1: Event Logging
- Measures: Monitor and log events for security purposes.

E. Communications Security

Control Objective: Secure internal and external communications.

- Control : A.13.1.1: Network Controls
- Measures: Manage and control networks to protect information based on business needs.

- Control : A.13.2.1: Information Transfer Policies and Procedures
- Measures: Establish secure procedures for data transfer.

F. Compliance

Control Objective: Ensure adherence to legal and regulatory requirements.

- Control : A.18.1.1: Identification of Applicable Legislation and Contractual Requirements
- Measures: Comply with legal and contractual obligations.

- Control : A.18.2.1 Independent Review of Information Security
- Measures: Conduct regular security reviews and audits.

2 . Applicability

List of ISO 27001 controls relevant to DHAEI based on the risk assessment and organizational needs.

- Access Control: Necessary due to the critical role in managing user access and authentication.

- Cryptography: Essential for protecting data confidentiality and integrity.

- Physical and Environmental Security: Needed to protect physical assets and infrastructure.

- Operations Security: Required to maintain secure and effective operation of IT systems.

- Communications Security: Important for securing data communications.

- Compliance: Ensures adherence to regulatory requirements and internal policies.

3 . Responsibility

- IT Security Manager: Responsible for implementing and maintaining access control and cryptographic measures.

- Operations Manager: Oversees operations security and monitoring.

- Facilities Manager: Ensures physical security and equipment protection.

- Compliance Officer: Manages compliance with legal and regulatory requirements.

4 . Monitoring and Review

Monitoring Procedures:

- Access Control: Regular audits and access reviews.

- Cryptographic Controls: Key management audits and encryption validation.

- Physical Security: Surveillance and access logs.

- Operations Security: Event logs and patch management reviews.

- Communications Security: Network traffic analysis and VPN security reviews.

- Compliance: Periodic compliance audits and policy reviews.

Review Frequency:

Monthly:

- Access control audits
- Patch management reviews
- Network security assessments

Quarterly:

- Cryptographic controls review
- Event logging analysis
- Physical security inspections

Annually:

- Compliance reviews
- Overall information security assessments

Conclusion

This Risk Management Plan for DHAEI provides a comprehensive framework to identify, assess, and mitigate risks associated with the organization's IT systems. By prioritizing and addressing these risks, DHAEI ensures the protection of its critical assets, maintains operational continuity, and upholds the confidentiality, integrity, and availability of its information.

References

1. National Institute of Standards and Technology (NIST). (n.d.-b). Data breach - glossary. CSRC. Retrieved August 6, 2024, from https://csrc.nist.rip/glossary/term/data_breach

2. Physical theft. (n.d.). Physical Theft - an overview | ScienceDirect Topics. Retrieved August 6, 2024, from https://www.sciencedirect.com/topics/computer-science/physical-theft

3. Defining insider threats: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). from https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

4. ISMS.online. (2022). Threat intelligence. ISMS.online. https://www.isms.online/iso-27001/annex-a/5-7-threat-intelligence-2022/

5. ISMS.online. (n.d.-b). ISO 27001:2022 annex A 8.12 – data leakage prevention. Retrieved August 6, 2024, from https://www.isms.online/iso-27001/annex-a/8-12-data-leakage-prevention-2022/#what-is-annex-a-8-12

6. ISMS.online. (n.d.). ISO 27001:2022 annex A 7.1 – physical security perimeters. Retrieved August 6, 2024, from https://www.isms.online/iso-27001/annex-a/7-1-physical-security-perimeters-2022/

7. ISMS.online. (n.d.). Annex A.9: Access Control. Retrieved August 6, 2024, from https://www.isms.online/iso-27001/annex-a-9-access-control/

8. ISMS.online. (n.d.). Annex A.10: Cryptography. Retrieved August 6, 2024, from https://www.isms.online/iso-27001/annex-a-10-cryptography/

9. ISMS.online. (n.d.). Annex A.11: Physical and Environmental Security. Retrieved August 6, 2024, from https://www.isms.online/iso-27001/annex-a-11-physical-and-environmental-security/

10. ISMS.online. (n.d.). Annex A.12: Operations Security. Retrieved August 6, 2024, from https://www.isms.online/iso-27001/annex-a-12-operations-security/

11. ISMS.online. (n.d.). Annex A.13: Communications Security. Retrieved August 6, 2024, from https://www.isms.online/iso-27001/annex-a-13-communications-security/

12. ISMS.online. (n.d.). Annex A.18: Compliance. Retrieved August 6, 2024, from https://www.isms.online/iso-27001/annex-a-18-compliance/