Risk Management Case Study

Prepared by: Mahad Mohamood

Date: August 5, 2024

Table of Contents

Overview

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 Assessment and Identification

The risk assessment process for DHAEI is structured to systematically identify and evaluate potential threats to the organization's IT assets. This involves:

1. Identifying Assets: Critical assets include :

- servers
- network infrastructure
- remote work setups

2. Identifying Vulnerabilities and Threats: Potential weaknesses and threats such as:

- Cyberattacks
- Data breaches
- Physical theft

3. Assessing Risks: Evaluating the likelihood and impact of each threat on the assets.

4. Determining Risk Owners: Assigning responsibilities for managing each identified risk.

Key Threats Identified:

1. Data Breaches:

- 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 another than authorized purpose."(NIST, Breach)
- Impact: Moderate to high, affecting the confidentiality and integrity of sensitive information.
- Likelihood: Moderate, given the existing controls.
- Effect on CIA: Confidentiality, Integrity.

2. Physical Theft:

- 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.).
- Impact: Moderate, primarily affecting the availability and confidentiality of physical assets.
- Likelihood: Lower compared to cyber threats.
- Effect on CIA: Availability, Confidentiality.

Challenges in Managing Threats:

- **Rapid Evolution of Threats:** Keeping pace with emerging cyber threats.
- **Resource Constraints:** Limited budget and personnel for implementing comprehensive security measures.
- **Integration of New Systems:** Ensuring new systems are secure and compliant with existing standards.

Risk Treatment Recommendations

To effectively mitigate the identified risks, the following treatments are recommended:

1. Data Breaches

- **Mitigations :**
  - Enhance data encryption
  - Enforce strict access controls
  - Conduct regular security training

- **Priority :** Medium, critical but less frequent than cyberattacks.

2. Physical Theft

- **Mitigations :**
    - Strengthen physical security measures
    - Use asset tracking systems
    - Implement secure storage practices
- **Priority :** Lower, given the reduced likelihood but still important for overall security.

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.

We encourage the management team and decision-makers to review the detailed Risk Management Plan document here to understand the strategic measures in place to secure our organization’s future.

References

1. National Institute of Standards and Technology (NIST). (n.d.-b). Data breach - glossary. CSRC. https://csrc.nist.rip/glossary/term/data_breach
2. Physical theft. Physical Theft - an overview | ScienceDirect Topics. (n.d.). https://www.sciencedirect.com/topics/computer-science/physical-theft