Risk Management
Case Study Report

Created by: Harsh Patel
Date: January 14, 2025

Table of Content

Purpose, Scope, and Users

The purpose of this Risk Management Plan is to provide DHAEI with a structured approach to identify, assess, and treat risks that may impact its operations, systems, and data. The scope of this plan covers DHAEI's head office, branch offices, remote workers, and digital assets, including Rackspace and AWS workloads. This plan is intended for use by executive management, the IT department, the Information Security team, and branch office IT support technicians.

Risk Assessment

The Process

The risk assessment process will follow a structured approach based on the NIST Risk Management Framework (NIST, n.d.). The steps include:

1. **Asset Identification**: Cataloging all critical assets.
2. **Threat Identification**: Using industry-recognized frameworks such as MITRE ATT&CK (MITRE, n.d.).
3. **Vulnerability Analysis**: Identifying weaknesses in systems and processes.
4. **Risk Determination**: Calculating risk based on impact and likelihood (ISO, 2019).
5. **Risk Prioritization**: Prioritizing risks for treatment.

Participants Involved:

- **Chief Information Security Officer (CISO):** Oversees the entire risk assessment process.
- **IT Support Technicians:** Provide insight into local systems and issues.
- **Branch Office Managers:** Help identify local operational risks.

Assets, Vulnerabilities, and Threats

Based on DHAEI's environment, the following are the key threats:

1. **Data Breaches** due to unauthorized access.
2. **Ransomware Attacks** targeting company servers and endpoints.
3. **System Downtime** due to hardware compromise or failure.

Challenges: Managing these threats involves ensuring endpoint security, maintaining encryption standards, and monitoring all critical infrastructure.

Determining the Risk Owners

The following chain of ownership will be established for risk management:

- **IT Support Technicians**: First-level risk owners responsible for identifying potential issues.
- **IT Manager**: Second-level owner who oversees risk mitigation.
- **CISO**: Final owner responsible for approving risk treatment strategies and reporting to the CEO.

Impact and Likelihood

Threat	CIA Impact (0-10)	Likelihood (0-5)	Description
Data Breach	C: 9, I: 9, A: 5	4	High impact on confidentiality and integrity.
Ransomware Attack	C: 8, I: 8, A: 7	3	Significant impact on availability.
System Downtime	C: 5, I: 3, A: 9	2	Major impact on availability.

Risk Acceptance Criteria

Risks with high impact and likelihood will be prioritized for treatment. Lower priority will be given to risks with minimal impact or low likelihood of occurrence. For example, system downtime may be minimized through redundancy and load balancing (ISO, 2019).

2.2 Risk Treatment

Summary of Threats and Mitigations

1. **Data Breach**
   - **Mitigation**: Implement MFA (Multi-Factor Authentication), endpoint encryption, and regular security audits (NIST, 2021).
   - **Priority**: High
2. **Ransomware Attack**
   - **Mitigation**: Deploy EDR (Endpoint Detection and Response) solutions, maintain regular backups, and conduct phishing awareness training (CISA, 2022).
   - **Priority**: High
3. **System Downtime**
   - **Mitigation**: Implement load balancing, clustering, and hardware monitoring.
   - **Priority**: Medium

Executive Summary

This Risk Management Plan for DHAEI outlines a detailed approach to identifying, assessing, and mitigating risks that may affect the organization's operations. Key threats identified include data breaches, ransomware attacks, and system downtime. The recommended treatments include implementing MFA, EDR solutions, and redundancy mechanisms. By following this plan, DHAEI can enhance its security posture and ensure business continuity.

References

Tactics - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/tactics/enterprise/

Risk management framework for information systems and organizations: (2018). https://doi.org/10.6028/nist.sp.800-37r2

Joint Technical Committee ISO/IEC JTC 1. (n.d.). *ISO/IEC 27005:2022(eN)*. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en

Cyber Essentials | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/resources-tools/resources/cyber-essentials

Barrett, M. P. (2020, January 27). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. NIST. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

Security and privacy controls for information systems and organizations. (2020). https://doi.org/10.6028/nist.sp.800-53r5