|  |  |  |
| --- | --- | --- |
| Group of people discuss something | | |
| Risk Management Case Study | | |
|  |  |  |
| By: Curtis Crawford | | |
| Table of Contents  **Executive Summary1**  Purpose, Scope, & Users2  Risk Assessment & Risk Treatment Methodology3  **Assets, Vulnerabilities, & Threats4**  Determining the Risk Owners5  Impact & Likelihood Table6  **Risk Acceptance Criteria7**  Risk Treatment8  Industry Standard Frameworks9  **References7**   |  | | --- | | Executive Summary |   DHAEI is a company specializing in software design and development. It’s digital footprint is expanding daily and the below risk assessment identifies cyber-attacks, data breaches and system downtime as the main threat the organization currently faces.  The negative impact on the confidentiality, integrity and availability of DHAEI’s systems requires prompt and persistent mitigation.  Mitigations for these risks might include installing software patches on a frequent basis, applying strong access controls on the system, encrypting sensitive data, including redundancy in the system, and having a disaster recovery plan in place. All these actions are prioritized based on how serious the risks are and the resulting probable impact on the organization.  With this implementation, DHAEI can strengthen its security posture, stay aligned with industry standards, and keep their digital assets and information safe from any cyber threats, thereby reinforcing further DHAEI’s profitable development and growth in its software development business. | | |
| Purpose, Scope, and Users | | |

Purpose:

The purpose of this paper is to put forward a complete framework for a risk assessment and risk treatment in the context of DHAEI – identify the risks, evaluate the impact and likelihood of each risk, and propose mitigations.

Scope:

All the IT assets, such as hardware, software, network systems and digital assets including the main office, branch offices and remote workers of DHAEI are within the scope of this report.

Users:

The main audience for this document will be the management at DHAEI, which includes the CEO, chief information officer (CIO) and other senior executives. The information security team, IT workers and support technicians will also use it to understand the risk and the suggested treatments.

|  |
| --- |
| **Risk Assessment and Risk Treatment Methodology** |

**Risk Assessment**

Process:

The risk assessment process for DHAEI involves the following steps:

Identify Assets:

List and categorize all IT assets including hardware, software, data, and personnel.

Identify Vulnerabilities and Threats:

Identify potential vulnerabilities in the system and the threats that could exploit these vulnerabilities.

Assess Risks:

Evaluate the impact and likelihood of identified risks. This involves qualitative and quantitative analysis.

Determine Risk Owners:

Assign ownership of each risk from ground level to senior executive level.

|  |
| --- |
| **Involved Individuals or Groups** |

CIO Amanda Wilson:

As the company’s IT director, Amanda will give strategic direction and help to keep IT in line with wider company objectives.

Paul Alexander (CISO):

Paul's team will perform detailed technical assessments and manage the security infrastructure.

William Freund (Manager of Systems):

William’s team will maintain the day-to-day ‘soup to nuts’ operations, and help the firm make sense of both the risks and the operational consequences.

|  |  |  |
| --- | --- | --- |
| Assets, Vulnerabilities, and Threats: | | |
|  |  |  |

Three Main Threats:

Cyber Attacks (e.g., Ransomware, Phishing):

Vulnerabilities: Outdated software, lack of user training.

Challenges: Ensuring timely updates and user awareness.

Data Breaches:

Vulnerabilities: Weak access controls, unsecured data storage.

Challenges: Implementing robust access control and encryption.

System Downtime:

Vulnerabilities: Hardware failures, inadequate backup systems.

Challenges: Ensuring redundancy and quick recovery mechanisms.

|  |  |  |
| --- | --- | --- |
| Determining the Risk Owners | | |
|  |  |  |

Cyber Attacks:

Ground Level: Security Technicians (e.g., Harold Fry)

Mid Level: CISO Paul Alexander

Senior Level: CIO Amanda Wilson

Feedback: The technicians responded to incidents and issues. The CISO managed security policy, while the CIO was in charge of strategically-directed security.

Data Breaches:

Ground Level: Systems Admin (e.g., Sy Truman)

Mid Level: Manager of Systems William Freund

Senior Level: CFO Rachel Xieng

‘Contribution:’ ‘Admins make sure data is accurate’ ‘Manager tries to ensure security;’ and ‘CFO reviews compliance, financial impact.’

System Downtime:

Ground Level: Support Technicians

Mid Level: COO Richard Xavir

Senior Level: CEO Alan Hake

Contribution: Technicians perform maintenance, COO manages operational efficiency, CEO ensures overall business continuity.

|  |
| --- |
| Impact and Likelihood Table: |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| **Risk Acceptance Criteria:** |

Cyber Attacks: High risk due to impact on confidentiality and integrity. Needs immediate and continuous attention.

Data Breaches: Critical due to potential regulatory and reputational damage. Requires robust security measures.

System Downtime: Significant but can be minimized with good redundancy practices.

|  |
| --- |
| **Risk Treatment** |

**Recommended Mitigations and Responses:**

Cyber Attacks:

Mitigations: Regular software updates, user training programs, multi-factor authentication.

Priority: High, due to frequent occurrence and severe impact.

Data Breaches:

Mitigations: Strong access controls, data encryption, regular security audits.

Priority: High, due to legal and financial implications.

System Downtime:

Mitigations: Redundant systems, regular backups, disaster recovery plans.

Priority: Medium, because while significant, it is manageable with proper procedures.

|  |
| --- |
| **Industry Standard Frameworks:** |

NIST Cybersecurity Framework: Provides guidelines on managing and reducing cybersecurity risks.

ISO/IEC 27001: Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS).

|  |
| --- |
| **References** |

* National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
* International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. <https://www.iso.org/standard/54534.html>
* ChatGPT – <https://chatgpt.com>
* Fortinet. Types of Cyber Attacks. (2023) – Top 20 Most Common Types of Cybersecurity Attacks. <https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks>
* Microsoft. (2023). Office 365. <https://www.microsoft.com/en-us/microsoft-365>
* Open Web Application Security Project. (2021). OWASP Top Ten. <https://owasp.org/www-project-top-ten/>
* Kaspersky. (2023). What is Ransomware? <https://www.kaspersky.com/resource-center/threats/ransomware>
* CISCO. (2023). Best Practices for Network Security. <https://www.cisco.com/c/en/us/solutions/enterprise-networks/borderless-networks/network-security.html>