

**Information Security Risk Assessment Report by Lead Risk Assessor Tremaine Hinds as of 29th May 2024.**

# Introduction

The purpose of this report is to present the findings of a risk assessment exercise carried out from [Feb 1] to [May 25th ] with the scope described below. The main purpose of the exercise was to assess the risks to [ThisIsAFakeCompany] and to identify which of these could be accepted and which may need some action to be taken to address them.

Once this risk assessment report has been approved, specific actions will be identified, discussed, agreed and then documented in a risk treatment plan to be managed as part of the Information Security Management System (ISMS).

The process used for this risk assessment is set out in the document Risk Assessment and Treatment Process which is part of the ISMS.

This risk assessment report describes:

* The context and scope of the risk assessment
* The assets within scope
* Threats to, and vulnerabilities of, those assets

This report is input to the risk treatment stage of the process and must be signed off by top management before continuing further.

This risk assessment was carried out by the following people:

|  |  |
| --- | --- |
| **NAME** | **ROLE IN ASSESSMENT** |
| Tremaine Hinds | Lead risk assessor |

*Table 1: Risk assessment team*

As part of the assessment, the following additional people were consulted:

|  |  |  |
| --- | --- | --- |
| **NAME** | **TITLE** | **LOCATION** |
| Shane Jones | Chief Technology Officer | Chicago office |
| Niccolo Sinckler | HR Manager | London office |

*Table 2: People consulted*

# Risk assessment context

This section describes the reasons why the risk assessment was carried out, the areas that were within its scope and the criteria that were applied in order to decide which risks are recommended for acceptance.

## Internal and external context

1. The Assessment was carried out to bolster Employee Safety and Well-being by Identifying and mitigating risks that could affect the safety and well-being of employees. This helps in creating a safe work environment, reducing the likelihood of workplace accidents and health issues. The aim was also to align risk management with the organization's strategic goals and objectives. This ensures that potential risks are considered in strategic decision-making, enhancing the likelihood of achieving business goals. Externally we aimed to remain up to date with technological advancements and managing risks associated with digital transformation and cybersecurity threats. This helps in leveraging technology while protecting the organization from cyber risks.

## Scope

This assessment aims to identify, analyze, and mitigate potential cybersecurity risks that could impact the information systems and data integrity of [ThisIsAFakeCompany] in order to data security, regulatory compliance, and protection against cyber threats. It does not cover risks to personal health or physical safety such as faulty equipment.

# Risk assessment results summary

**Rating Scale:**

Impact:

High (H): This would result in severe consequences, such as significant data loss, extended downtime, or large financial penalties.

Medium (M): This could cause moderate disruption, such as data corruption, partial system outage, or reputational damage.

Low (L): This would have minimal impact, such as minor data loss, brief system disruption, or minor inconvenience.

Likelihood:

High (H): This event is very likely to occur within a reasonable timeframe (e.g., frequent hardware failures, common security vulnerabilities).

Medium (M): This event could occur occasionally (e.g., occasional power outages, potential for human error).

Low (L): This event is unlikely to occur (e.g., highly secure systems with strong access controls, rare natural disasters).

**Risk Assessment Matrix**

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | Threat | Threat Level & Impact | Mitigation Strategies |
| Servers & Data Centers | Service Disruption | H (Hardware failure, power outage) | Redundant hardware, UPS (Uninterruptible Power Supply), backup generator |
| Servers & Data Centers | Unauthorized access | VH (Cyberattack) | Strong passwords, access controls, intrusion detection systems |
| Servers & Data Centers | Data Loss | VH (Fire, natural disaster, cyberattack) | Backups, disaster recovery plan |
| Security Software | Spread of Malware | M (Outdated software) | Security software with regular updates, user training |
| Security Software | Intentional Sabotage | M (Rogue employee with access) | User activity monitoring, access controls |
| Security Software | Erosion of Trust | L (Minor software glitch) | Transparency about software limitations |
| Policies and Procedures | Operational Disruption | M (Lack of clarity) | Clear and concise policies, easy access for employees |
| Policies and Procedures | Inefficiency | M (Unnecessary procedures) | Review and streamline policies regularly |
| Policies and Procedures | Confusion and Errors | M (Lack of training) | User training and awareness programs |
| Data Transmission | Man-in-the-Middle (MitM) Attacks | VH (Unencrypted data) | Encryption (VPN, TLS) |
| Data Transmission | Data Leakage and Eavesdropping | VH (Unsecured network) | Network segmentation, data encryption |
| Data Transmission | Financial Loss | VH (Financial data breach) | Strong data security practices, compliance with relevant regulations |
| Response Plans | Inadequate Planning and Preparation | H (Unfamiliar with procedures) | Develop and test incident response plans, training for staff |
| Response Plans | Resource Wastage | M (Inefficient recovery process) | Streamline recovery procedures, conduct resource allocation assessments |
| Response Plans | Ineffective Response | VH (Unclear communication) | Clear communication plan for stakeholders during incidents, training for staff on response procedures |

 **Threats to Servers & Data Centers are rated highly** due to the critical nature of the data they store and the potential for severe disruptions.

 **Data Transmission threats are all rated Very High** due to the sensitive nature of the information being transmitted and the potential for financial losses.

This makes servers and data centres and data transmission, the assets with the highest risk associated with them.

## ASSET-BASED ASSESSMENT

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REF** | **ASSET** | **TYPE (P/F/S)** | **THREAT** | **ADDITIONAL COMMENTS** |
| 1 | Servers & Data Centers | P | * Service Disruption * Unauthorized access * Data Loss | Physical and virtual servers, storage systems, and data center operations |
| 2 | Security Software | F | * Spread of Malware * Intentional Sabotage * Erosion of Trust | Antivirus, anti-malware, firewalls, and intrusion detection/prevention systems |
| 3 | Policies and Procedures | F | * Operational Disruption * Inefficiency * Confusion and Errors | Acceptable use policies, data handling procedures, and security protocols |
| 4 | Data Transmission | F | * Man-in-the-Middle (MitM) Attacks * Data Leakage and Eavesdropping * Financial Loss | Encryption protocols, secure communication channels, and data transfer processes |
| 5 | Response Plans | F | * Inadequate Planning and Preparation * Resource Wastage * Ineffective Response | Incident response procedures, communication plans, and recovery strategies |

*Table 3: Risk assessment results summary (asset-based)*

*Figure 1: Asset-based risk assessment*