*Summary Report - Module 4*

*Top Ten Risks Summary Report*

Version *1.5*

Prepared By: *John Doe [Your Name Here]*

Date: *06/01/2019*

VERSION HISTORY

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version #** | **Implemented**  **By** | **Revision**  **Date** | **Approved**  **By** | **Approval**  **Date** | **Reason** |
| 1.0 | Kim Fang | 05/20/18 | Kyle Green | 05/28/18 | Document creation |
| 1.5 | John Doe | 05/20/19 | Kyle Green | 05/28/19 | Updated top ten risks & employment of new preparer of document (John Doe) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

TABLE OF CONTENTS

[1 Introduction 4](#_Toc487790192)

[1.1 Purpose 4](#_Toc487790193)

[2 Executive Summary 4](#_Toc487790194)

[3 Detailed Summary 4](#_Toc487790195)

[3.1 *Risk Evaluation section of Risk Register* 4](#_Toc487790196)-5

[3.2 *Accounting data is hacked due to ransomware*  5](#_Toc487790197)

[3.3 *Economic crises*  6](#_Toc487790198)

[3.4 *Safety policy complications*  6](#_Toc487790197)

[3.5 *Weak privilege and access control*  6](#_Toc487790198)

[3.6 *Weak password policy* 6](#_Toc487790198)

[3.7 *Poor network monitoring*  6](#_Toc487790197)

[3.8 *Bad front-end coding*  7](#_Toc487790198)

[3.9 *Improper training on data access*  7](#_Toc487790198)

[3.10 *Employee turnover*  7](#_Toc487790197)

[3.11 *Bad software QA tests*  7](#_Toc487790198)

[3.12 *Notable non-top ten risks*  7](#_Toc487790198)

[4 Recommendations 8](#_Toc487790199)

[5 SuggEstED aCTIONS 9](#_Toc487790200)-10

[Appendix A: Approval 11](#_Toc487790201)

[APPENDIX B: REFERENCES 12](#_Toc487790202)

[APPENDIX C: KEY TERMS 13](#_Toc487790203)

# 

# Introduction

## Purpose

This Summary Report provides a summary of the top ten identifiable risks, which are capable of impacting XYZ Technology Services.

# Executive Summary

XYZ Technology Services is using this Summary Report to inform employees about the top ten risks threatening the company. The detailed summary provides the risk prioritization number (RPN) for each operational risk. Moreover, this section also thoroughly describes the top ten risks and why they are so dangerous. At the end of the detailed summary is a list of notable non-top ten risks. The top ten risks to the company can change in the future, depending on the most hazardous threats to the company.

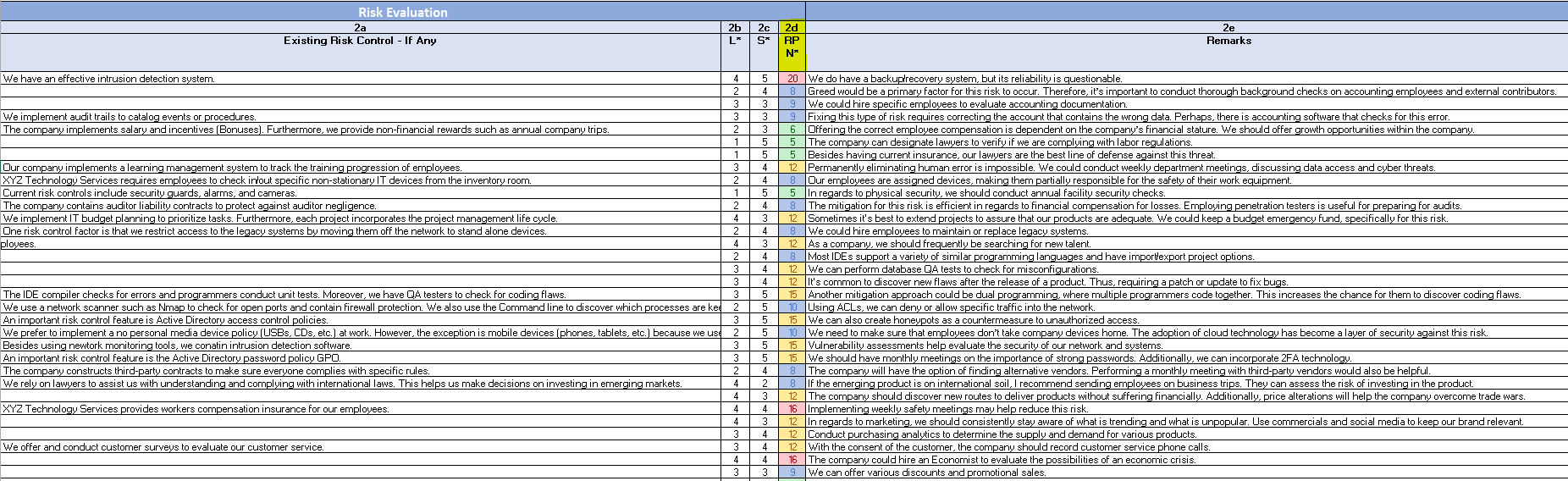
Implementing mitigation procedures is the main recommendation within this Summary Report. Additionally, XYZ Technology Services should consider conducting risk assessment meetings. The suggestive tasks in this Summary Report incorporate mitigation approaches for the current top ten risks. Ignoring to recognize and reduce our vulnerabilities is reckless behavior, which we will not accept!

# Detailed Summary

## *Risk Evaluation section of Risk Register*

XYZ Technology Services requires risk evaluation to calculate the risk prioritization number. Using the risk formula (Likelihood \* Impact), we can determine the RPN. The likelihood of a risk occurring is on a scale of one to five, with five being the highest chance of occurrence. Similarly, the impact is on a scale of one to five, with five being the greatest impact.

***Image of the Likelihood and Impact of Operational Risks***



***Image of Risk Matrix***

## 

## *Accounting data is hacked due to ransomware (#1 risk)*

Ransomware is a malicious piece of software, intentionally preventing users from accessing their systems or important files. Scareware, screen lockers, and encrypting ransomware are the three main types of ransomware. In regards to accounting, this risk would be devastating because it would prevent Accountants from accessing, documenting, and processing financial transactions. Furthermore, the company could pay a hefty fee to cybercriminals to regain access to our systems or personal files. **This type of threat receives a severity level of twenty!** Ransomware has become one of the most common malware attacks, making it a great concern for any company, with valuable data. The occurrence of this risk has the potential to cripple the company, costing us millions of dollars.

## *Economic crises (#2 risk)*

The economy is an essential piece of a nation, providing financial stability. However, economic problems can happen, with the ability to financially hinder an entire country. These economic issues can include credit, fiscal, currency, and hyperinflation. **Why does this risk receive a severity level of sixteen?** Mainly because we cannot prevent the occurrence of an economic crisis. This is because of the political factors, which contribute to economic conflicts. Our company and customers would suffer from economic threats. Consumers would alter how they spend money due to the need to survive. Likewise, XYZ Technology Services would change how we price, market, create and invest, to protect the health of our company.

## *Safety policy complications (#3 risk)*

Safety first is not just a saying at XYZ Technology Services. We pride ourselves in providing a safe work environment for our employees. The company is aware that work accidents will happen, such as physical injuries, which can be big or small. **Therefore this risk receives a severity level of sixteen.** In the result of a horrible work accident, we could experience high employee turnover rates or excessive lawsuits. Without a safe work environment, the company’s overall productivity will decline. Moreover, failing to comply with safety policies could result in a company shutdown.

## *Weak privilege and access control (#4 risk)*

Strict employee access policies through Active Directory (AD) are vital for reducing unauthorized access. Weak privilege and access control is a dangerous risk, especially for XYZ Technology Services. If unauthorized users access important system data, we can experience numerous problems. For example, the deletion or theft of sensitive data can occur due to weak privilege and access control. **This type of threat receives a severity level of fifteen!** The likelihood of this risk is occasional (3), but the impact is reasonably at a five.

## *Weak password policy (#5 risk)*

Enforcing a strong password policy through AD is a crucial layer of security against cybercriminals. An example of a strong password policy is setting alphanumeric passwords with a minimum length of eight. A weak password policy would leave passwords vulnerable to cracking. **This type of threat receives a severity level of fifteen!** XYZ Technology Services must protect usernames and passwords because these are the credentials employees rely on for accessing company systems. In the wrong hands, the company could experience identity theft, malware infections, and theft of intellectual property. Recovering from this risk would be a complex matter, requiring an abundance of time and money.

## *Poor network monitoring (#6 risk)*

Network professionals monitor the network traffic for any anomalies. These events could be the beginning of a cyber-attack! Therefore, poor network monitoring hurts the company’s security efforts to protect our systems. **The risk of poor network monitoring receives a severity level of fifteen!** Threats would slip past the eyes of our Network Administrators, and Security Analysts. Undetectable activity passing through XYZ Technology Services network may contribute to future data breaches.

## *Bad front-end coding (#7 risk)*

Software developers should code with functionality and security in mind. Bad front-end coding is a programming risk, which can impact the security of our web applications. **Why does this risk receive a severity level of fifteen?** Mostly, because the impact of bad front-end coding is at five. Vulnerable front-end applications allow consumers and malicious individuals to manipulate our applications. XYZ Technology Services cannot guarantee that the intentions of these users will be genuine. Consequently, this risk endangers the company’s data and customer credentials.

## *Improper training on data access (#8 risk)*

Many companies stress the importance of employee training, educating them on the dangers of technology. Improper training on data access would invite cyber-attacks such as phishing and ransomware into the workplace. **This risk easily receives a severity level of twelve!** The likelihood of this risk is occasional due to human error (forgetfulness, negligence, misinformation, etc.), but the impact can be devastating. At XYZ Technology Services, training on data access is one of our countermeasures for mitigating cyber threats. If we begin to experience an abundance of technological risks, improper employee training would be one of the reasons why.

## *Employee turnover (#9 risk)*

Employees are the heart of XYZ Technology Services. They develop, manufacture, market, and much more. A high turnover rate is worthy of being on the list of top ten risks. **Specifically, this type of risk receives a severity level of twelve!** We try our best to accommodate our employees, but we are aware that employees will leave for various reasons. This risk can damage the company’s reputation, productivity, and team chemistry. So, it’s important to implement mitigation tactics to protect the company’s future.

## *Bad software QA tests (#10 risk)*

QA (Quality Assurance) Testers are watchful experts, who check our products for flaws. Moreover, they are one of the last lines of defense against threats to our products. Bad software QA tests could create numerous issues for XYZ Technology Services. For example, end-users could receive a product which doesn’t function correctly due to bugs. **This risk easily receives a severity level of twelve!** While the likelihood is occasional, the impact is at four. End-users could discover the flaws within our applications and perform exploitations. The occurrence of this risk puts our reputation and products in jeopardy.

## *Notable non-top ten risks*

Below are additional risks, with reasonable severity levels, which didn’t make the list of top ten risks.

***Budget risk (Severity level of 12)***

***Tariff wars (Severity Level of 12)***

***Brand risk (Severity Level of 12)***

***Database configuration risk (Severity Level of 12)***

***Supply & demand issues (Severity Level of 12)***

***Poor customer service (Severity Level of 12)***

# Recommendations

XYZ Technology Services should urgently plan for mitigation procedures against the top ten risks within this Summary Report. Furthermore, this should be the responsibility of the risk assessment team. They can reference the **Risk Register version 1** document, examining the remarks for protecting against threats. I think the company should also begin conducting monthly meetings, in regards to new or old risks which may obtain a spot on the top ten rankings. This will help the company determine how efficient their risk management strategies are; while promoting security awareness within the workplace.

# SuggEstED aCTIONS

***Accounting data is hacked due to ransomware (#1 risk)***

* Promote security awareness (Ransomware training)
* Backup sensitive data

***Economic crises (#2 risk)***

* Hire an Economist to assess the current state of the economy
* Executives should build a healthy relationship with the government
* Executives should build a healthy relationship with media entities
* Develop a company emergency economic fund for investing
* Construct new facilities in other nations in case of economic problems

***Safety policy complications (#3 risk)***

* Promote workplace safety (Training)
* Make sure we have Workers Comp Insurance
* Employ Safety Supervisors

***Weak privilege and access control (#4 risk)***

* Promote security awareness (Weak privilege and access control training)
* Maintain AD access control policy

***Weak password policy (#5 risk)***

* Promote security awareness (Weak password training)
* Maintain AD password policy
* Conduct password penetration tests against employee passwords (Dictionary attack, Brute Force attack, etc.)

***Poor network monitoring (#6 risk)***

* Promote security awareness (Network Monitoring training)
* Make sure network monitoring tools are updated and relevant
* Conduct penetration tests against Network Administrators (Network Sniffing)

***Bad front-end coding (#7 risk)***

* Promote secure programming (Front-end coding security training)
* Implement dual employee programming (Team programming)

***Improper training on data access (#8 risk)***

* Promote security awareness (Data access training)
* Conduct ethical hacking against various departments

***Employee turnover (#9 risk)***

* Promote a healthy work culture
* Improve compensation packages
* Continue to scout for new talent

***Bad software QA tests (#10 risk)***

* Promote QA testing training
* Implement dual employee QA testing
* Create an additional QA testing team for final approvals

Appendix A: Approval

The undersigned acknowledge they have reviewed the aboveand agree with the approach it presents. Changes to this will be coordinated with and approved by the undersigned or their designated representatives.

|  |  |  |  |
| --- | --- | --- | --- |
| Signature: | Generated signature | Date: | 05/28/2019 |
| Print Name: | Brent Tucker |  |  |
| Title: | CEO |  |  |
| Role: | The CEO makes the final decision on major corporate decisions. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Signature: | Generated signature | Date: | 05/28/2019 |
| Print Name: | Gary Bishop |  |  |
| Title: | CISO |  |  |
| Role: | The CISO is responsible for determining what security features the company needs. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Signature: | Generated signature | Date: | 05/28/2019 |
| Print Name: | Ira Dixon |  |  |
| Title: | Risk Assessment Manager |  |  |
| Role: | The Risk Assessment Manager confirms and evaluates all risks to the company. |  |  |

APPENDIX B: REFERENCES

The following table summarizes the documents referenced in this document.

|  |  |  |
| --- | --- | --- |
| **Document Name and Version** | **Description** | **Location** |
| **Risk Register version 1** | The Risk Register is a risk assessment form. This form contains risk identification data, risk evaluation data, and risk control information. | C:\Users\Gamer1\Desktop\Security Risk Assessment |
| **Malwarebytes. (2019).** | This document describes ransomware is detail. | <https://www.malwarebytes.com/ransomware/> |
| **Pettinger, T. (2010).** | This document provides information about various economic issues. | <https://www.economicshelp.org/blog/2294/economics/economic-problem/> |
| **Oxford University Press. (2019).** | This document describes fiscal. | <https://en.oxforddictionaries.com/definition/fiscal> |
| **Amadeo, K. (2019).** | This document discusses hyperinflation. | <https://www.thebalance.com/what-is-hyperinflation-definition-causes-and-examples-3306097> |
| **Techopedia, Inc. (2019).** | This document describes Active Directory. | <https://www.techopedia.com/definition/25/active-directory> |

APPENDIX C: KEY TERMS

The following table provides definitions for terms relevant to this document.

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Ransomware | Ransomware is a type of malware that denies users access to their systems or important files. |
| Fiscal | Fiscal relates to money, taxes, debts, and other numerical assets, which belong to the government. |
| Hyperinflation | Hyperinflation is the event when prices increase at a rapid rate as money decreases in value. |
| Active Directory | Active Directory is a Windows OS directory service providing unification for network resources. |
| Brute Force Attack | A Brute Force Attack is a hacker method for obtaining access to anything with password protection. This attack aggressively tries combinations of usernames and passwords until it breaks in. |
| Dictionary Attack | A Dictionary Attack is a hacker method for obtaining access to anything with password protection. This attack attempts to guess passwords using a word-list. |
| Phishing | Phishing is a hacker technique useful for gathering personal information. This commonly occurs through suspicious emails or infected websites. |