# Final Report

# IT Risk Management

ROUTINE
PROTOCOL

Prudhvi Sai Nikith Kodavati

Professor: Joseph Murdock

It Risk Management- ISMG 6980

17-December-2022

**Executive Summary:** This current Report provides an overview of the risk management strategy within the context of Routine Protocol. However, it is a provider of computer products and accessories. This organisation has developed an online retail initiative in response to intense competition. However, risk management is essential for the development of a safety technique in every project. In contrast, technical risk is the organization's primary concern as it develops an online marketing approach. Reviewing the risk requires that a company employ remedial strategy and action. In this study, both quantitative and qualitative risk analysis techniques should be undertaken by examining risk registers, incident responses, and a few other comparable businesses.

**Risk Management in Routine Protocol:**

The process of detecting, evaluating, and mitigating potential risks to the assets and profits of an organisation is referred to as risk management. These dangers might originate from a wide number of places, such as unpredictability in the financial sector, potential legal repercussions, challenges posed by emerging technologies, oversights in strategic management, unfortunate events, and catastrophic natural occurrences. An effective risk management programme enables a company to think about the full scope of the dangers to which it is exposed. In risk management, the relationship between risks and the influence that risks could have on an organization's strategic goals is also investigated, as is the possibility that risks could have a cascade effect. Five steps are Identify the risks. Analyze the likelihood and impact of each one. Prioritize risks based on business objectives. Treat the risk conditions. Monitor results and adjust as necessary.

**Risk Register:**

Risk 1: Potential for a data breach of sensitive customer information located on various (electronic) company resources.

- **Risk description** – Network-accessible employees, suppliers, and consultants can risk data. They can access your data via network, email, mobile devices, and the cloud if your firm has it. Perimeter security doesn't protect data. Insiders compromise data. Emails or phishing websites can install malware and steal passwords. Your cloud provider's employees can lose, hack, or corrupt data. Data breach victims must determine who has jurisdiction. Tis may lose the stakeholder's trust which finally results in loss of fundings.
- **Affected assets** – Assets like names, residences, phone numbers, email addresses, birth dates, and schooling. Legal processes and comments on the company's business methods should also be documented. Architecture, encryption keys, user names, and passwords
- **Risk score** - Medium
- **Risk treatment analysis** – Risk analysis can be done with what kind of information was involved, who the data was stolen from or shared with, if they were able to access or view the data, and what steps were done to mitigate the damage.
- **Risk treatment-** I would like to suggest Lexical analysis It uses regular expressions to recognise structured data like SSNs, credit card numbers, medical terms and geographical information in papers. Snort, an open source network IDS, permits custom signatures and regular expressions. It compares intercepted packets to these signatures and rules to detect data leaks.

Risk 2: Potential for a disruption to the physical retail locations where customers would not be able to visit or make purchases from these 2 locations.

- **Risk description:** The proliferation of shopping done online presents several challenges. Customers stand to benefit from purchasing online. There is a possibility that the pricing found online and in-store are very different. The fact that these two retail locations probably won't accept customers is a physical disruption. We continue to peruse and then switch between categories without understanding that we have spent hours on this site. Before making a purchase, you might want to do some research on the reputation of the firm and read some reviews from previous customers. The upkeep of in-store inventories has a significant impact on this risk.
- **Affected assets**: Retail Disruption, Reduced sale of products, Impact on Customer Satisfaction, Brand Name and Loss of incomes
- **Risk score :** Low
- **Risk treatment analysis**: Alter the product based on the comments and suggestions of customers, the current state of the market, the many different options available, and the extensive range of products..
- **Risk treatment**: I would suggest innovating the commodity in adherence to current market trend and offering a number of different alternatives. Also, enforce advertising campaigns and branding to attract a large number of customers. I would suggest modernising the product in keeping with current trends and offering a number of different options. Bringing the mode of transactions up to date will ensure that they are processed quickly.

Risk 3 Potential for a catastrophic disruption at the denver location which would render the data center unavailable, causing an interruption to all locations, including the online presence.

- **Risk description:** The possibility of a disastrous event taking place at the Denver location, which could lead to the data centre being ordered to cease operations as a result. This would have an influence on all of the locations, including the presence that can be found online. This may directly lead to the failure of the server, the network, the storage system, or even the entire data centre.
- **Affected assets:** Company's data, Personnel Records, Administration, E-commerce website.
- **Risk score :** Medium
- **Risk treatment analysis**: When tenacity is utilised, a server, network, cloud service, or even a whole data centre will be able to recover rapidly and continue operations in the event that there is a disruption caused by a failure of the equipment, a loss of power, or another type of disturbance.
- **Risk treatment**: It is highly recommended by me that the planning and maintaining data centres, data centre managers should design data centre specifications in an accurate and reasonable manner, taking into account data security, power, capacity, efficiency, and other related issues, and using a DCIM system and virtualization technology to improve data centre operational efficiency.

## Incident response playbook- Phishing

**Purpose:** To respond quickly to phishing. We must observe certain procedures and rules. This document outlines how to recognise, evaluate, and resolve a phishing issue.

1. **Planning:**

- Review and implement policies for handling cyber incidents, including technical and business responsibilities, and escalate if necessary.
- Regular security training should be provided for employee data that is private, confidential, or highly dangerous.

2. **Detection:**

- Investigate a data breach or compromise using both automatic and manual detection channels.
- Social media outlets for customers and employees should be investigated with phishing emails with links from internal and external notices

3. **Initiation:**

- Recognize a fraudulent email by its type of cyberattack, number of employees who received the phishing email, cause for hacking, initial implications, and current activities.
- Gather evidence for further inquiry, such as copies of the dangerous programme and forensic copies of the infected computer.

4. **Analysis**:

- Analysis of scope, and its impact while Checking to discover if any tainted property has been recalled and quarantined.
- Determine if any credentials have been hacked and the company's impact.

5. **Eradication:**

- Mitigate the attack's effects. Use automatic or manual tools to fight phishing attempts.
- Before distributing new data backups, reinstall any independent OS backups.

6. **Recovery:**

- We must ensure all affected systems are secure and calculate costs and damages.
- Change affected employees' usernames and passwords once identified. If the impacted points include smartphones, immediately execute the "Remote Wipe" command to remove any sensitive information/data on them.

7. **Remediation:**

- Always ensure sure your servers, workstations, and wireless devices and servers have the latest software upgrades/patches and antiphishing software.
- In a phishing assault, humans are always affected first, then IT Infrastructure when login info is stolen.

8. **Closure:**

- Once the eradication, recovery and remediation is completed. Then the next step is closure.

**Three companies that provide IT risk management/security program management services that can assist the company.**

**1. Company name:** Venseca

- **Location:** Pennsylvania, United States
- **Website:** https://www.venseca.com/
- **Summary of services provided:** Venseca makes it possible for an organisation to easily assess the risk that is posed by a third-party vendor by utilising an algorithm that is protected by a provisional patent.
- **Reason why you are proposing this company as an option:** The accuracy of fraud detection is improved with each new transaction, which is one reason why I select Venseca. Before making any conclusions regarding the safety of transactions, it is necessary to go through millions of data points. This enables online retailers to identify irregularities and reduce the likelihood of incurring financial hazards.

**2.Company name:** Strategic Risk Associates

- **Location:** Virginia, United States
- **Website:** https://www.srarisk.com/
- **Summary of services provided:** SRA provides risk management, M&A, banks, and consulting services to financial institutions. Watchtower ERM dashboard provides executive and board-level reporting on KRI/KPIs, risk appetite management, strategic objectives tracking, peer performance, policy limits, and regulatory examination management. It's a single, integrated solution to manage risk, boosting decision-making and performance.

- **Reason why you are proposing this company as an option:** My decision to go with SRA was based on the fact that they offer innovative threat protection, data security, intrusion prevention, encryptions, information systems, and cloud security as part of their regulatory examination management in addition to tracking strategic objectives, peer outcomes, policy limits, and regulatory compliance evaluations.

**3.Company name:** CyberSecOp

- **Location:** Newyork, United States
- **Website:** https://cybersecop.com/security-risk-management-services
- **Summary of services provided:** Compliance services include PCI, Sarbanes-Oxley, HIPAA, NIST, and General Data compliance. Protection Regulation Governance, risk, and compliance (GRC) consulting and implementation services, helping deploy leading GRC technology to support compliance decision making.
- **Reason why you are proposing this company as an option:** CyberSecOp was my first choice due of their round-the-clock customer support. Their risk management and prevention strategies are the best in the business, according to the reports. Also provides services in third-party risk management, which aid in the formulation, implementation, and oversight of third-party risk management initiatives.

**References:**

Team, CloudMask. "Data Breaches: Threats and Consequences." *Cloudmask*, https://www.cloudmask.com/blog/data-breaches-threats-and-consequences.

Nadkarni, Anirudh. *Breach Risk Analysis: A Four-Step Plan*. blog.24by7security.com/breach-risk-analysis.

Boughton, Bobby. "How to Mitigate and Respond to Data Breaches." *Converge*, 19 July 2018, convergetechmedia.com/how-to-mitigate-and-respond-to-data-breaches.

Peacock, Justin. *Risk Register Examples for Cybersecurity Leaders*. www.cybersaint.io/blog/risk-register-examples-for-cybersecurity

Tucci, Linda. "What Is Risk Management and Why Is It Important?" *Security*, 12 Oct. 2021, www.techtarget.com/searchsecurity/definition/What-is-risk-management-and-why-is-it-important.