Report-Risk Management

Leonardo Oliveira Pereira
University of Coimbra, Department of Informatics Engineering, Portugal
uc2020239125@student.uc.pt

1 Introduction

Following the risk management frameworks and methodologies, this assignment focus understand the process of analyzing, evaluating, and planning risk management activities for the retail company. The multifaceted nature of the retail business, embracing diverse functionalities such as business information storage and sharing, supply chain support to multiple stores, client's information storage, and employee information handling, requires a well planned approach.

This risk management plan include the following steps: **system categorization**, including system description, boundaries definition, and the risk tolerance analysis, **risk identification and assessment**, including asset valuation, threat assessment, vulnerability assessment, and **risk control strategies**, including examples of security controls to implement, and a monitoring and re-assessment plan. By meticulously categorizing systems, evaluating potential risks, and formulating effective control measures, this plan seeks not only to mitigate existing vulnerabilities but also to prepare the organization for potential future threats.

2 System Categorization

2.1 System Description

In the context of the retail company's multifaceted operations, the system categorization process involves a meticulous examination of its digital and physical components.

- **Physical Components**
  - **Management and Control Center:** Building that holds the management centralized system.
  - **Supply Chain Infrastructure:** Warehouses, delivery vehicles, and inventory storage facilities.
  - **On-Premises Systems:** Multiple stores, geographically distributed, each with its own set of networked devices, point-of-sale systems, and storage system.
- **Digital Components**

- **Web Application:** Online platform where clients purchase products. It incorporates secure payment gateways and encrypted communication protocols.
- **Centralized Management System:** Software responsible for supply chain operations and centralized information storage.
- **Employee Information Storage:** Stores details of managers, technical personnel, and other staff, ensuring role-based access controls.
- **Client Information Storage:** Contains payment data, delivery addresses, personal data, and purchase history. Data encryption are applied to safeguard sensitive information.

2.2 Boundaries definition

Boundaries are established to delineate the extent of the system's influence and interaction. These boundaries define the scope of the system and specify what is included and excluded from management activities and risk assessments.

Similarly to the previous one, boundaries are set digital and physical components.

- **Physical Boundaries**
  - **Management and Control Center:** Restricted to authorized personnel only and houses data centers.
  - **Supply Chain Infrastructure:** Includes warehouses, delivery vehicles, and inventory storage areas.
  - **On-Premises Systems:** Limited to the geographical locations of the stores and their immediate surroundings.
- **Digital Boundaries**
  - **Web Application**: Interaction limited to customer transactions and order processing.
  - **Centralized Management System:** Manages centralized storage and processing of client information, payment data, and employee records.
  - **Employee Information Storage:** Accessible only to authorized personnel for human resources and administrative purposes.
  - **Client Information Storage:** Accessed for order processing and customer support, joining to stringent access control policies.

2.3 Risk Tolerance Analysis

Risk tolerance (or Risk Appetite) is a fundamental concept that sustains the decision-making process regarding the level of acceptable risk in pursuit of organizational objectives. In this context, the retail company demonstrates a balanced approach, acknowledging the inherent risks in the retail industry while prioritizing the security of client data, financial transactions, and supply chain integrity. The organization is committed to maintaining compliance with industry standards, ensuring customer trust, and safeguarding its reputation.

The risk tolerance is made up of by the following levels:

- **High Risk Tolerance**
  - **Strategic Decisions:** High tolerance for risks associated with strategic decisions, innovation, and market expansion.
  - **Operational Agility:** Willing to accept a certain degree of operational risks for the sake of flexibility and agility.
  - **Adaptability:** Embracing risks as opportunities for growth and adaptation to changing market demands.
- **Medium Risk Tolerance**
  - **Operational Efficiency:** Balanced approach, emphasizing operational efficiency without compromising fundamental security and compliance.
  - **Customer Data Security:** Medium tolerance for risks related to customer data security, ensuring robust encryption and access control measures.
  - **Supply Chain Optimization:** Willingness to explore innovative supply chain solutions while maintaining supply chain integrity and transparency.
- **Low Risk Tolerance**
  - **Financial Transactions:** Low tolerance for risks concerning financial transactions and compliance. Adherence to strict financial security protocols and regulatory compliance.
  - **Customer Trust:** Non-negotiable in customer data protection, implementing the highest industry standards for data encryption and privacy.
  - **Reputation Management:** Zero tolerance for risks affecting brand reputation, with a focus on proactive measures to prevent any negative publicity.

3 Risk Identification and Assessment

3.1 Asset Valuation

Identification, valuation and categorization of information systems assets are critical tasks of the process to properly develop and deploy the required security control for the specified IT assets. Organizations or individuals able to implement security for assets by using this model must first identify and categorize the organization's IT assets that need to be protected in the security process.

In the context of the retail company, the following assets were identified:

- **A1-Physical Store:** On-Premise System, geographically distributed, with its own set of networked devices, point-of-sale systems, and storage system.
- **A2-Online Store:** Online platform where clients purchase products.
- **A3-Employee's Information:** Contains details of managers, technical personnel, and other staff.

- **A4-Client's Information:** Contains payment data, delivery addresses, personal data, and purchase history.
- **A5-Business Information:** Includes data related to the company's operations, sales, inventory, financial records.
- **A6-Supply chain support:** Comprises physical assets such as warehouses, transportation vehicles, and inventory.
- **A7-Management and control center:** Main core responsible for supply chain operations and centralized information storage
- **A8-Plan/Strategy for Marketing:** Marketing department that includes all the plans and strategies for advertisement.

After identifying the assets, it is important to do the asset valuation (figure 1) that is the weight scored of each asset which results from the calculation of the impact to revenue, impact to profitability and impact to public image. The weight for the impact to profitability is higher due to the nature of the business in which an positive balance is the main focus, the other impacts shares the same weight because they are thought to be of equal importance.

The values on the follow figure were assigned on the basis of personal opinion.

ID Asset	Information Asset	Criterion 1: Impact to Revenue	Criterion 2: Impact to Profitability	Criterion 3: Impact to Public Image	Weighted Score
	Weights	*30*	*40*	*30*	*100*
A1	Physical Store	1	0.9	0.9	93
A2	Online Store	1	0.9	0.9	93
A3	Employee's Information	0.5	0.5	0.7	56
A4	Client's Information	0.6	0.6	0.6	60
A5	Business Information	0.8	0.6	0.5	63
A6	Supply chain support	0.8	0.5	0.1	47
A7	Managment and control center	0.7	0.9	0.5	72
A8	Plan/strategy for Marketing	0.8	0.8	1	86

Figure 1: Asset Valuation

The weighted score is higher for the assets A1, A2 and A8 because these assets are those who interact directly with customers and make the company generate money. A8 has the higher impact to public image due to its nature focusing on the marketing field while the A1 and A2 assets have higher impact to revenue and profitability because it is where the payment operations enters the field.

A little bit lower weighted score belongs to A7 that has a strong impact on both revenue and profitability but not that much impact to public image due to lack of direct interaction with the clients.

Finally the other assets, A3, A4, A5 and A6, have the lowest weighted score thanks to the fact that they deal with the logistics side of the business. Assets A3 and A4 focus on personal data information and that is why they have a medium impact to revenue and profitability, analogously, asset A4 has the same impact to public image comparing to

the other impacts, but asset A3 has a little bit higher impact to public image since the employee information is important to the company and clients. Finally, for the assets A5 and A6 he have stronger impact on impact to revenue, similar impact as the two assets mentioned before and lower impact to public image, especially the A8 asset, all thanks to their main focus on the logistics side of the business such as data operations, sales, inventory, warehouses, and delivery vehicles.

3.2 Threat and Vulnerability Assessment

A general list of threats should be compiled, which is then reviewed by those most knowledgeable about the system, organization or industry to identify those threats that apply to the system.

For this work, a considerable number of threats have been identified, not to demonstrate that they are the most correct or the main ones, but rather that they are just examples of possible threats to the business in question.

So, the general list of threats comes in the next figure 2:

Threat	Threat	Example
T1	Electrical Spike	Interruption of electrical power, or electrial spikes
T2	Natural Disasters	Earthquakes, floods, hurricanes
T3	Fire	Electrical fires, arson, wildfires
T4	Physical Damage	Accidental damage by employees or clients
T5	Security Breaches	Theft, vandalism, unauthorized access, terrorism, counterfeit currency
T6	CyberSecurity Breaches	Data breaches, malware, phishing attacks, information disclosure of confidential or private planning documents
T7	Insider Threats	Employees with mailicious purposes
T8	Reputation Threats	Negative publicity
T9	Supply chain Disruptions	Problems with suppliers or delivery services
T10	Third-party risks	External vendors, suppliers, or partners who might have access to sensitive data or systems
T11	Retail Competition	Competitors selling similar or cheaper clothes, stronger advertising by competitors

Figure 2: Threats examples

After mentioning threats and identifying a few of them, it is important to be more specific and speak about vulnerabilities.

Vulnerabilities refer to weaknesses or flaws in a system's design, implementation, or operation that can be exploited by attackers to compromise the system's security. These weaknesses can exist in various components, such as software, hardware, networks, or organizational processes. Exploiting vulnerabilities can lead to unauthorized access, data breaches, system malfunctions, or other security incidents. Identifying and patching vulnerabilities is crucial for maintaining the security and integrity of systems and data.

For the risk management it is relevant to identifying vulnerabilities because it enables organizations to understand their risks, take proactive measures to mitigate these risks,

comply with regulations, optimize resources, make informed decisions, and continuously improve their security posture.

Having said that, the figure 3 shows the vulnerabilities to the threats set out above:

Threat ID	Threat Description	Vulnerability	Possible Vulnerabilities
T1	Electrical Spike	V1	Lack of surge protection
		V2	Lack of failure prediction system
T2	Natural Disasters	V3	Building without seismic protection
		V4	Building without glass windows protection
T3	Fire	V5	Lack of fire extinguishers
		V6	No Fire Detection System
T4	Physical Damage	V7	Lack of security protocols (No emergency exit, no safety map)
		V8	No slippery floor warning
T5	Security Breaches	V9	No anti-theft system
		V10	No security system (security cameras, alarm)
T6	CyberSecurity Breaches	V11	No policies for data operations
		V12	No backup system
T7	Insider Threats	V13	No background checks
		V14	No vigilance/logging system
T8	Reputation Threats	V15	No quality control system
		V16	No satisfaction control system (reply to clients feedback online)
T9	Supply chain Disruptions	V17	Geopolitical issues
		V18	No tracking system
		V19	Lack of diversification
T10	Third-party risks	V20	Inadequate Access Controls
		V21	Insecure Data Transmission
		V22	Insufficient Due Dilligence
T11	Retail Competition	V23	Market Saturation
		V24	Ineffective Marketing
		V25	Inflexible Pricing Strategies

Figure 3: Vulnerabilities examples

3.3 Threat and Vulnerability Assessment(TVA)

A Threat and Vulnerability Assessment (TVA) is a comprehensive evaluation of an organization's information security infrastructure. It involves identifying, quantifying, and prioritizing security vulnerabilities and assessing potential threats in order to determine the risks they pose to the organization. Here's how the process typically works:

1. **Identifying Assets:** The first step in TVA involves identifying all the assets within an organization that need to be protected. These can include physical assets (like computers and servers), software, data, networks, facilities, and even human resources.

2. **Identifying Vulnerabilities:** Vulnerabilities can exist at various levels, including software, hardware, networks, and human processes.

3. **Identifying Threats:** Threats are potential dangers that can exploit vulnerabilities in assets. Threats can come from various sources, including malware, malicious employees, natural disasters, electric spike, and more. During a TVA, analysts assess the likelihood and impact of these threats occurring and explore potential scenarios in which vulnerabilities could be exploited.

4. **Analyzing Risks:** Risks are evaluated by combining the likelihood of a threat exploiting a vulnerability with the impact it would have on the organization. This analysis helps in prioritizing which vulnerabilities need to be addressed urgently. High likelihood and high impact vulnerabilities are typically the most critical and require immediate attention.

By following this steps, organizations can better understand their security posture, prioritize their security efforts, and make informed decisions to protect their valuable assets from potential threats.

Once all these steps have been taken, the result of the TVA table is shown in the figure 4, displayed immediately below.

		Physical Store	Online Store	Employee's Information	Client's Information	Business Information	Supply chain support	Managment and control center	Plan/strategy for Marketing		
		A1	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**	**A8**		
Electrical Spike	**T1**	V1 V2					V1	V1 V2			
Natural Disasters	**T2**	V3 V4						V3			
Fire	**T3**	V5 V6					V5	V5 V6			
Physical Damage	**T4**	V7 V8						V7			
Security Breaches	**T5**	V9 V10					V10	V10			
CyberSecurity Breaches	**T6**		V11 V12	V11 V12	V11 V12	V11 V12	V11 V12	V11 V12	V11 V12		
Insider Threats	**T7**	V13 V14	V13 V14	V13 V14	V13 V14	V13 V14	V13 V14	V13 V14	V14		
Reputation Threats	**T8**	V15	V15 V16					V15	V15 V16		
Supply chain Disruptions	**T9**					V19	V17 V18 V19	V19			
Third-party risks	**T10**	V20	V20 V21	V20 V21	V20 V21	V20 V21 V22	V22	V20 V21 V22	V20 V21 V22		
Retail Competition	**T11**	V23	V23					V24	V23 V24 V25		
	number of vulnerabilities	15	9	6	6	8	11	17	11		
	Priority of Controls	1	less priority	2		3		4		5	higher priority

Figure 4: TVA table followed by the number of vulnerabilities on each column and the range of the priority of controls

Looking at the table, certain spaces with the respective vulnerabilities have different colours according to the priority of the controls. These green colours of different shades come from the analysis of the inherent risks.

The different shades of colour associated with each of the spaces and their respective vulnerabilities were based on the following values:

- Level 1 - 0 up to 20%
- Level 2 - 20 up to 40%
- Level 3 - 40 up to 60%

- Level 4 - 60 up to 80%
- Level 5 - 80% or higher

To reach the value ranges mentioned above, a risk analysis was carried out based on a ranked vulnerability risk. The risk value is evaluated by combining a series of metrics such as **asset value**, **likelihood**, **attack success probability**, **loss frequency**, **probable loss**, **loss magnitude** and **uncertainty**.

These metrics are defined as follows:

1. **Asset Value:** value resulting from asset valuation step.
2. **Likelihood:** probability that the vulnerability in the organization is a target of an attack.
3. **Attack success probability**: probability of the attack being executed with success.
4. **Loss frequency:** calculation of the likelihood of an attack coupled with the probability of its success.
5. **Probable Loss:** percentage of asset value loss if attacked.
6. **Loss Magnitude:** value of the asset that might be lost in an attack.
7. **Uncertainty:** percentage of compensation due to probability estimation.

Finally, after assigning values to each of the metrics based on own intuitions, the risk value is calculated. Figure 5 shows the risk analysis for Asset A1 and then the same process will be applied to the other assets in a similar way.

Asset	Asset Relative value	Vulnerability	Loss Frequency			Loss Magnitude (Impact)			Uncertainty	Risk
			Likelihood	Attack	Loss	Asset Value	Probable	Loss		
A1	93	V1	20%	80%	16%	93	10%	9.3	70%	2.5296
A1	93	V2	20%	80%	16%	93	10%	9.3	70%	2.5296
A1	93	V3	10%	90%	9%	93	100%	93	30%	10.881
A1	93	V4	10%	90%	9%	93	100%	93	30%	10.881
A1	93	V5	15%	90%	14%	93	100%	93	60%	20.088
A1	93	V6	15%	90%	14%	93	100%	93	60%	20.088
A1	93	V7	15%	80%	12%	93	20%	18.6	70%	3.7944
A1	93	V8	20%	20%	4%	93	5%	4.65	30%	0.2418
A1	93	V9	90%	95%	86%	93	95%	88.35	10%	83.093175
A1	93	V10	90%	95%	86%	93	95%	88.35	10%	83.093175
A1	93	V13	50%	90%	45%	93	80%	74.4	60%	53.568
A1	93	V14	50%	90%	45%	93	80%	74.4	60%	53.568
A1	93	V15	70%	70%	49%	93	60%	55.8	20%	32.8104
A1	93	V20	80%	90%	72%	93	90%	83.7	15%	69.3036
A1	93	V23	90%	85%	77%	93	90%	83.7	30%	83.23965

Figure 5: Ranked Vulnerability Risk for Asset A1

By conducting a Threat and Vulnerability Assessment (TVA), organizations can better understand their security posture, prioritize their security efforts, and make informed decisions to protect their valuable assets from potential threats.

4 Risk Control Strategies

Risk control strategies are methods and approaches used by organizations to manage, mitigate, or eliminate risks identified through risk assessment processes. These strategies aim to minimize the impact and likelihood of risks occurring, ensuring that the organization can operate effectively and achieve its objectives.

For this part of the risk management only the most assets with higher priority of controls visible in figure 4 were considered, i.e. the assets A1, A2, A5, A7, A8. The assets are backed by selective descriptive controls and the corresponding metrics as it is presented in the figure 6. Emphasising that the information in the next figure has been made up of own intuitions and that there may be missing more control strategies.

Assets	Selected Control	Selected Metric
A2 - Online Store A5 - Business Information A7 - Managment and control center A8 - Plan/Strategy for Marketing	Defence - Document/implement/monitor policies for data operations (authentication, encryption)	Cost of implementation (price of HW, price of SW) Cost of maintenance (costs with equipment, goods, ...) Number of attacks attempts detected Number of attacks attempts unsuccessful Number of attacks successful
A1 - Physical Store A7 - Managment and control centers	Defence - (Protection products/building) Acquire the fire detection system	Cost of the implementation of the fire detection system (FDS) (cost of equipment and service provisioning) Cost of annual maintenance Level of Accuracy and how fast the system performs detection in an accurate way (e.g. false positives) Number of incidents Number of working days (i.e., not having the impact to close doors
A1 - Physical Store A7 - Managment and control center	Defence - (Protection products/building) Acquire Fire Extinguishers	Cost of equipment Cost of maintenance Cost of training Number of products that are protected Number of incidents Easiness of usage after training and rapid reaction from coworkers
A1 - Physical Store A2 - Online Store A7 - Managment and control center A8 - Plan/Strategy for Marketing	Defence - Analyse the market and monitor competitors' strategies	Cost of research and analysis Cost of maintenance Impact on sales and revenue Impact on customer retention rate
A1 - Physical Store A7 - Managment and control center	Defence - Acquire security system (anti-theft, security cameras, alarm)	Cost of equipment Cost of implementation Cost of maintenance Number of incidents Number of features supported (e.g., able to connect to Information system to trigger an alarm in a map)
A1 - Physical Store A2 - Online Store A5 - Business Information A7 - Managment and control center A8 - Plan/Strategy for Marketing	Defence - Clearly Defined Contracts	Cost of lawyers Percentage of contracts with defined security clauses Compliance rate with regulatory requirements
A1 - Physical Store A2 - Online Store A8 - Plan/Strategy for Marketing	Implement satisfaction control system (reply to clients feedback online)	Cost of implementation Cost of maintenance Number of opinions Feedback rate
A1 - Physical Store A2 - Online Store A5 - Business Information A7 - Managment and control center A8 - Plan/Strategy for Marketing	Defence - Implement vigilance/logging system	Cost of implementation Cost of maintenance Number of attacks attempts detected Number of attacks attempts unsuccessful Number of attacks successful

Figure 6: Controls strategies

Effective risk control strategies can involve a combination of these approaches, tailored to specific situations and types of risks. Organizations must regularly review and update their risk control strategies to adapt to changing environments and emerging threats.

5 Impact of a Malicious attack on the Management and Control Center

A malicious attack on the management and control center affect the normal operation of the stores. Two distinct scenarios are proposed, each reflecting a varying magnitude of intrusion.

First Scenario: Limited Intrusion

In this scenario, the attacker gains partial access to our Management and Control Center. While the breach is detected and contained swiftly, its impact echoes through the succeed operations operations:

- **Store Operations Disruption:** Some stores might experience temporary disruptions in inventory management and supply chain operations. Customer transactions could be slowed down, affecting customer experience and sales.
- **Reputation Damage:** News of the incident might reach customers, denting our reputation temporarily.

Controls and secure measures:

- **Vigilance/logging system:** Real-time Vigilance/logging system detects the intrusion early, allowing swift containment.

Second Scenario: Severe Intrusion

For this scenario, the attacker gains extensive access to our Management and Control Center, potentially compromising critical systems:

- **Widespread Data Breach:** Extensive customer data, including payment information and personal details are compromised.
- **Store Paralysis:** Stores across the network experience severe disruptions. Point-of-sale systems falter, inventory management collapses, and supply chains grind to a halt. Customer transactions are paralyzed.

Controls and secure measures:

- **Redundant Systems:** Redundant systems and data backups ensure quick recovery and minimal data loss.
- **Advanced Encryption:** Implementation of advanced encryption protects sensitive customer data.

In both scenarios, the controls and security measures play a deciding role. Early Vigilance/logging system not only minimize operational disruption but also indicates dedication to customer security. The implementation of advanced encryption and redundant systems fortifies the robustness, ensuring that even in the face of a severe attack, the ability to recover and rebuild remains unwavering.

6 Conclusion

The endurance of a robust risk management plan cannot be overstated. The risk management, adapted for the retail company with geographically dispersed stores, a centralized control center, and a thriving online presence, has been a challenge.

The report began with a system categorization, where the nuances of digital and physical components were meticulously dissected. Defining clear boundaries and articulating our risk tolerance levels was crucial.

Ventured deeper into the realms of risk, the analysis revealed the vulnerabilities and potential threats faced by the retail company. Precious assets were identified each requiring a bespoke protection against the risks ahead. The vigilance and foresight exercised in the risk assessment were a testament to security and resilience.

Armed with this knowledge, we charted our course through risk control strategies. Encryption, access controls, strict compliance protocols, and strategic partnerships emerged as sentinel guardians. The implementation of security measures was not merely an obligation but a pledge to the clients – a promise of safety in every transaction, online interaction, and in-store experience.

In conclusion, the risk management plan stands as a testament to a commitment to innovation, customer trust, and unwavering integrity. It can been see as a shield, protecting our operations, our customers, and our legacy.

Link to access the google sheet!