Report - Risk Management Assignment

Francisco Catarino Mendes - 2019222823
Department of Informatics Engineering
University of Coimbra

1 Context

This report contains a risk management plan for a retail company. Throughout this paper, the enterprise will be subject to a system categorization, that includes a system description, a determination of its boundaries, and a risk tolerance analysis, followed by risk identification, assessment, and control strategies, with the help of various frameworks that help us manage risk.

In the end, an effectiveness discussion will be needed in order to decide if the risk management plan was built accordingly, by way of giving examples of attacks and how they would be dealt with.

2 Definitions

1. Asset - items that have value.
2. Asset Valuation - allows to determine the overall importance an enterprise places on each asset.
3. Vulnerability - a weakness that could be exploited to cause loss or harm.
4. Threat - a set of circumstances that could cause harm.
5. Harm - the negative consequence of an actualized threat against a vulnerability.
6. Control - prevents threats from exercising vulnerabilities.
7. Policy - a formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.
8. Standard - detailed statements of what must be done to comply with policy.
9. Practice/Guideline/Procedure - explains how to comply with policy.
10. Risk - the probability for harm to occur, or of loss or injury.
11. Quantitative Assessment - an analysis using actual values or estimates.
12. Qualitative Assessment - an analysis using an evaluation process based on characteristics using non-numerical measures.
13. Risk Framing - establishing the context and providing a common perspective on how organizations manage risk.
14. Risk Appetite/Tolerance - the level of risk or degree of uncertainty that is acceptable to organizations based on trade-offs.
15. Residual Risk - the risk to information assets that remains even after current controls have been applied.

16. Boundaries - the security perimeter of what is being protected, covering all the components of an information system.
17. Risk Identification - the recognition, enumeration, and documentation of risks to an organization's information assets.
18. Risk Assessment - a determination of the extent to which an organization's information assets are exposed to risk.
19. Risk Control - the application of controls that reduce the risks to an organization's information assets to an acceptable level.
20. Risk Management - the process of identifying risk, assessing its relative magnitude, and taking steps to reduce it to an acceptable level.
21. Likelihood - the probability that the vulnerability in the organization is a target of an attack.
22. Attack Success Probability - the probability of the attack being executed with success.
23. Probable Loss - the percentage of asset value loss if attacked.
24. Uncertainty - the percentage of compensation due to probability estimation.
25. Loss Frequency = Likelihood * Attack Success Probability
26. Loss Magnitude = Asset Value * Probable Loss
27. Relative Risk Assessment: Loss Frequency * Loss Magnitude - Percentage of risk mitigated by current controls + Element of uncertainty
28. Defense - Attempt to prevent exploitation of the vulnerability.
29. Mitigation - Attempt to reduce the impact of an attack rather than reduce the success of the attack itself.
30. Single Loss Expectancy (SLE) = Asset Value x Exposure Factor
31. Annualized Loss Expectancy (ALE) = SLE x Annualized Rate of Occurrence
32. Cost-Benefit Analysis = ALE(prior control implementations) - ALE(post control implementations) - Annualized Cost of Safeguard

3 System Categorization

This section of the report is heavily influenced by the NIST Risk Management Framework for Information Systems and Organizations, NIST SP 800-37. It is composed of Task P-11, Authorization Boundary, and Task P-12, Information Types, of the Prepare Step, and the Categorize Step, which includes the system description and the security categorization.

3.1 System Description and Architecture

In regard to the architecture, the company is structured by a management and control center, responsible for supply chain operations and centralized information storage, multiple stores geographically distributed, and then an online store system, from which the clients can make their requests.

The informatics system handles business information storing and sharing, which includes enterprise details like stock, partners, and types of products, among others, supply chain operations, by way of communicating with the suppliers and the stores, client information storage, such as client cards, name, e-mail, preferences, and so on, and also employee information, similar to background, salary, shifts, etc. Moving on to physical assets, one must consider the vehicles used when supplying the stores, the infrastructures, the products, and the different sorts of individuals (employees, employers, clients).

Furthermore, the system already has some security functionalities in place, those being network segmentation, access control policies, confidentiality policies, contingency plans, individual accountability, auditors, alarms, video vigilance, good practices in coding, recovery controls, detection mechanisms, and user authentication.

3.2 System Boundary

To begin with, a list of the technical assets is needed. The business has hardware and firmware, software, cross-domain devices and requirements, network connection rules, interconnected information systems, and encryption techniques, among others. Moreover, infrastructure, personnel, and equipment can also be put in the mix.

Then, the authorization boundaries can be defined. They must englobe all the key components for the good functioning of the company. Firstly, here is one regarding the points of sale, or physical stores:

1. Hardware and equipment;
2. Personnel;
3. Infrastructures;
4. Data and Network Connections

Another boundary that can be set is regarding the informatics systems:

1. Network Infrastructures;
2. Web Application and other software;
3. Servers and Data Centers;
4. Security Controls/Mechanisms;

Together, the technical assets information and the authorization boundaries information form the system boundary, which is fundamental for the rest of this report.

3.3 Information Types

Concerning the information types the system deals with, these were the ones considered to be relevant:

1. Unclassified Information - information that can be publicly available, like general product information.
2. Sensitive but Unclassified Information - information that is public, but needs protection, like sales performance figures.
3. Confidential Information:
   (a) Financial Information - private data, such as supplier contracts and general transactions.
   (b) Personal Identifiable Information (PII) - data subject to data protection regulations, like name, addresses, etc.
   (c) Intellectual Property - propriety information, like trademarks, that needs protection.
   (d) Research Data - information about market or product developments, according to client preferences.

3.4 Security Categorization

With the system boundary and information types defined, as well as a system description, the next step is categorization. A security category is the characterization of information or a system based on an assessment of the potential impact on organizational operations and assets should there be a loss in confidentiality, integrity, or availability (security objectives) of such information or system.

For each information type described earlier, a category (low, medium, or high) is going to be given to the security objectives, that represents the impact level on the enterprise, should they be compromised. Table 1 shows the result of this procedure:

Information Types	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Unclassified Information	Low	Medium	High
Sensitive but Unclassified Information	Low	Medium	Medium
Financial Information	Medium	Medium	Low
Personal Identifiable Information (PII)	High	Low	Medium
Intellectual Property	Medium	Medium	Low
Research Data	High	Medium	Low

Table 1: Security Categorization

The generalized format for expressing the security category, SC, of an information type is:

SC = (confidentiality, impact), (integrity, impact), (availability, impact)

As for the security impact level for a system, it is determined by taking the maximum impact value of the system's security category – that is, of the three security objectives for each information type and security category.

3.5 Risk Tolerance Analysis

To provide a complete system categorization, a risk tolerance analysis for the business is also needed. By evaluating the type of compliance requests and sensitive data that exist, it is determined if taking some risks is worth it. Also, with the help of the system categories defined in the previous section, trade-offs are determined, using a comparison between confidentiality, integrity, and availability so that it can be known how to make decisions in cases of clashes since one compromise might be more tolerable than the other.

3.5.1 Risk Tolerance Level

Starting with the risk tolerance level, it is established here as ”Medium Tolerance”. Due to the fact that a retail company has some policies to comply with, and handles various types of sensitive data, the ”High Tolerance” level possibility gets put aside immediately. As for the reason why a ”Medium Tolerance” level description is being chosen over a ”High Tolerance” level description, the fact is that some strategic objectives are too important to be compromised by a more effective level of security, like the performance of the entire informatics system, or the research processes being conducted to gain an advantage in the area. Even so, stability maintenance must be always one of the priorities, and a reassessment of this measure can lead to a decrease in the risk tolerance level.

3.5.2 Priorities and Trade-Offs

Following once more the data gathered from the security categorization done earlier, it is clear that ”High” security categories are the ones that must have priority in case of a failure of the system since those would be the most impactful to the organization. Below are the trade-offs that could be made in more detail:

1. Confidentiality vs Availability: when, for example, the channel reliability that ensures the availability of the web application is low, action must be taken to ensure access at all times, because going offline can result in disaster, economically and in terms of reputation and satisfaction of the customer. But doing that might expose the always present need for confidentiality of client and company information. The same goes when inverting the roles, and a simple example is locking an account as a result of entering the wrong credentials. While this may protect identity and data theft, it directly impacts the availability of the system. So, for a retail company, it might be better for the focus to be a little more on the side of availability, as it is the main pillar of the business, but not to the point of increasing dangerously the probability of data leaks that could have great consequences.

2. Confidentiality vs Integrity: one can say that these two go hand-in-hand. They both are directly affected by authorization. That being said, authorization levels must be carefully attributed to prevent wrongful access or changes to data. Depending on the roles inside the organization, the trade-offs happen when deciding the permissions of that same role. While one of the pillars might be affected, it might be necessary so that the other one is not compromised and the role does not gain unintended access.

3. Integrity vs Availability: this relationship is similar to the one that availability has with confidentiality. Once again, the battle is between granting access and restricting access. For example, the informatic system of the company might be using a backup to compensate for a reliability failure. This event causes harm to integrity, as it becomes easy for an attacker to enter the system through the backup. On the other hand, false alarms related to integrity protection could cause the system to become unavailable, without a realistic reason. As a retail company, availability is the primary goal. And as we see in the system categorization, integrity failures never have a massive impact on the organization. That being said, availability should be prioritized in most cases against integrity.

4 Risk Identification

4.1 Assets and Asset Valuation

Before giving the list of assets and their respective weights, a definition of criteria and default weights is needed, on a scale of 0-100.

Criterion 1: Impact on Revenue (30);

Criterion 2: Impact on Profitability (30);

Criterion 3: Impact on Public Image (40).

For each criterion, a score between 0-1 is going to be given to the asset. Then, by multiplying the two scores, the final weight is obtained.

(a) A1 - Products/Inventory: 1x30 + 1x30 + 1x40 = 100, products are arguably the most important asset of all, therefore they get the maximum score in all criteria;

(b) A2 - Building and Equipment: 0,6x30 + 0,6x30 + 0,9x40 = 72, the infrastructure and equipment will have an influence in the costumer's opinion, not so much in the revenue and profitability;

(c) A3 - Staff: 0,5x30 + 0,5x30 + 0,7x40 = 58, once again, public image is the most affected, due to the fact that interactions between staff and clients can change the reputation of the organization;

(d) A4 - Information Management System: 0,7x30 + 0,7x30 + 0,7x40 = 70, this asset is relevant to all aspects, because without it the company would not be able to function at all;

(e) A5 - Strategic Planning (Investors, Partnerships, Types of Products): 0,7x30 + 0,8x30 + 0,8x40 = 77, this one affects profitability and public image most due to the fact that if our partners have good reputation, it will only benefit the enterprise, as well as having in stock well-known to the public types of products;

(f) A6 - Transport Vehicles: 0,3x30 + 0,3x30 + 0,5x40 = 38, transport vehicles are not that relevant, only criterion they can have some impact is the public image due to the fact that the transportation and the vehicles are visible to everyone;

(g) A7 - Plan/Strategy for Marketing: 0,7x30 + 0,8x30 + 1x40 = 85, the marketing plan is one of the most important assets a company can have, and has huge influence on its public image.

4.2 Threat Identification

(a) T1 - Electrical Spikes (interruption of electrical power, or electrical spikes);

(b) T2 - Natural Disaster (earthquakes, floods, hurricanes);

(c) T3 - Fire (electrical fires, arson, wildfires);

(d) T4 - Physical Damage (accidental damage by staff or visitors, structural failures);

(e) T5 - Security Breaches (theft, vandalism, unauthorized access, terrorism);

(f) T6 - CyberSecurity Breaches (data breaches, malware, phishing attacks, information disclosure of confidential or private planning documents);

(g) T7 - Insider Threats (staff or Organization Individuals with malicious purposes);

(h) T8 - Reputation Threats (negative publicity, competition);

(i) T9 - Supply Chain Disruptions (disruptions in the Management Center);

4.3 Vulnerability Identification

(a) T1: Lack of surge protection (V1); Lack of failure prediction system (V2);

(b) T2: Building without seismic protection (V3); Not doing regular maintenance and evaluation of the building (V4);

(c) T3: Lack of fire extinguishers (V5); No Fire Detection System (V6);

(d) T4: Lack of warning signs (V7); Staff training and education (V8);

(e) T5: Lack of security detection in the products to prevent theft (V9); Weak doors and windows (V10);

(f) T6: No policies for data operations (V11); No backup system (V12);

(g) T7: No background checks (V13); No vigilance/logging system (V14);

(h) T8: No quality control system for products (V15); Not keeping up to date with market evolution (V16);

(i) T9: No response plan/system/policies (V17); Lack of a track down system of transport vehicles (V18);

4.4 TVA Table

For the priority of controls, the TVA relationships considered to be most critical are:

1. Vulnerabilities related to fire that can affect products, because the consequences could be massive;
2. Vulnerabilities related to physical damage that can affect products, because a huge lack of mistreatment of the products can lead to bad events;
3. Vulnerabilities related to cybersecurity breaches that can affect the information management system, due to the fact that if the whole system of the organization becomes compromised, the consequences could be big and unpredictable;

4. Vulnerabilities related to insider threats that can affect both the strategic and marketing planning, since if someone with bad intentions manages to get inside the company, both plans can be altered and integrity becomes compromised;

5. Vulnerabilities related to supply chain disruptions that can affect inventory, due to the fact that if something fails in the supply chain, it could originate critical lack of products overall.

		Products/Inventory	Building and Equipment	Staff	Information Management System	Strategic Planning (Investors,	Transport Vehicles	Plan/Strategy for Marketing			
		A1	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**			
Electrical Spike	**T1**		V1 V2		V1 V2						
Natural Disasters	**T2**	V3 V4	V3 V4	V3 V4	V3 V4		V3 V4				
Fire	**T3**	V5 V6	V5 V6	V5 V6	V5 V6		V5 V6				
Physical Damage	**T4**	V7 V8	V7 V8	V8			V8				
Security Breaches	**T5**	V9 V10	V10								
CyberSecurity Breaches	**T6**				V11 V12	V11 V12		V11 V12			
Insider Threats	**T7**	V14	V14	V13 V14	V13 V14	V13 V14	V14	V13 V14			
Reputation Threats	**T8**					V15 V16		V15 V16			
Supply Chain Operations	**T9**	V17 V18			V17	V17	V18				
	number of vulnerabilities	11	10	7	11	7	7	6			
	Priority of Controls	1	less priority	2		3		4		5	higher priority

Table 2: TVA Table

5 Risk Assessment

In this section, using the information from the TVA Table, it is made clear which vulnerabilities influence which assets. Then, with that data, for each vulnerability, the loss frequency and the loss impact are calculated, the first one by defining the likelihood and the attack success probability and the second one by using the asset value and determining the probable loss. Finally, by giving uncertainty a value, all the components needed will be known to determine the relative risk. In Table 3, the process for asset 1 is shown. The full table is available in the spreadsheet linked at the end of the document.

Moreover, this is where some assumptions are made. They are the following:

(a) Retail Company is based in a metropolitan area;

(b) Vulnerabilities can occur on a year basis;

(c) Probability of natural disasters occurrence: 5%;

(d) Probability of occurrence of fire: 20%;

(e) Retail Company has high reputation.

Asset	Asset Relative value	Vulnerability	Loss Frequency			Loss Magnitude (Impact)			Uncertainty	Risk
			Likelihood	Attack Success Prob.	Loss Freq	Asset Value	Probable Loss	Loss Magnitude		
A1	100	V3	5%	50%	3%	100	100%	100	80%	4.5
A1	100	V4	5%	50%	3%	100	100%	100	80%	4.5
A1	100	V5	20%	70%	14%	100	100%	100	90%	26.6
A1	100	V6	20%	70%	14%	100	100%	100	90%	26.6
A1	100	V7	50%	50%	25%	100	5%	5	30%	1.625
A1	100	V8	20%	60%	12%	100	20%	20	40%	3.36
A1	100	V9	50%	80%	40%	100	5%	5	50%	3
A1	100	V10	30%	70%	21%	100	50%	50	70%	17.85
A1	100	V14	50%	70%	35%	100	40%	40	60%	22.4
A1	100	V17	30%	80%	24%	100	30%	30	40%	10.08
A1	100	V18	30%	80%	24%	100	30%	30	40%	10.08

Table 3: Vulnerability Risk for Asset 1

6 Risk Control Strategies

(a) Defense - Acquire a fire detection system: Assets A1, A2, A3;

(b) Defense - Acquire Fire Extinguishers: Assets A1, A2, A3;

(c) Defense - Put in place warning signs: Assets A1, A2;

(d) Mitigation - Implement a track-down system for the transportation vehicles: Assets A1, A6;

(e) Defense/Mitigation - Educate staff: Assets A1, A2, A6;

(f) Defense - Document/implement/monitor policies for data operations (authentication, encryption): Assets A4, A5, A7;

(g) Defense - Implement backup mechanisms: Assets A4, A5, A7;

(h) Defense - Do background checking: Assets A4, A5, A7;

(i) Defense - Acquire a vigilance system/adopt logging policies: Assets A4, A5, A7;

(j) Mitigation - Implement a quality control system: Assets A5, A7;

(k) Defense - Do research on market evolution: Assets A5, A7.

Using the TVA Table, it was possible to define which relations between threats, assets, and vulnerabilities had more priority in regard to having control strategies for them. The above are the controls that were created by applying that knowledge.

Each of the controls uses a number of metrics to judge their own performance. Those can be seen in the spreadsheet linked at the end of the document.

After implementing the controls, when reassessing this risk management plan, a cost-benefit analysis will be possible, which will determine along with the metrics if the controls implemented were successful or not.

7 Effectiveness discussion and final remarks

With the risk management plan finished, the only process left is to give examples of attacks and how this plan would deal with them. The imaginary situations are the following:

1. An error made by an employee when doing database operations regarding inventory, affecting integrity and supply chain operations;
2. A decrease in sales and reputation due to unknown reasons.

The first scenario triggers two controls, one that makes sure that the staff is re-educated so that this type of error does not happen again, and one that creates more policies regarding data operations to ensure that the modifications intended are correct. As for resolving the supply chain error, for example, the control that implements a track-down of the transportation vehicles can be used to redirect them. Even so, the impact of an error like this can still be of great effect to the corporation.

In the second example, the controls that get activated are doing (more) market research, in order to understand what went wrong and also to analyze the competition's latest actions, and also implementing a quality control system, because the decrease in sales could be associated with the quality of the products being poor, that can result in a downgrade to the reputation. The impact of something of this order can also be significant, as sometimes it takes time to understand what is wrong with the actual state of the company.

To sum up, this document contains a risk management plan for a retail company, that shall be used whenever the organization needs it, which means that whenever there is a risk to the enterprise, it should be scrutinized by this plan. It goes without mention that a constant reassessment of this plan should be made, to re-evaluate the state of the organization.

Link for Risk Management Spreadsheet:

`https://docs.google.com/spreadsheets/d/1DRXfAw_66Eb6yRb2FQiLzX5k3aCBKixj/edit?usp=sharing&ouid=105633069300502448317&rtpof=true&sd=true`