LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Security risk analysis in retail store,

Case study: Company X

Nugrahany, Raihana Darmiati

2015 Leppävaara

Security risk analysis in retail store, Case study: Company X

Raihana Darmiati Nugrahany
Security Management
Bachelor's Thesis
January, 2015

Laurea University of Applied Sciences **Abstract**
Leppävaara
Security Management

Raihana Darmiati Nugrahany

Security Risk Analysis in retail store, Case study: Company X

Year 2015 Pages 49

This thesis was conducted to protect the valuable assets of the case study company. By using the risk analysis, it will improve their business resilience by being well organized to prevent the occurrence of the threats and taking appropriate measure as response to it and by applying corporate security it can help to manage the safety of business function and assets of the case company.

The purpose of this study is to identify various type of external and internal risk in the case company through risk identification. By identifying the risk, it helps the company to prepare themselves from various risks that might disturb their business operation. After the risk has been identified then the authors analyze the risk by analysing the risk form its impact and frequency of occurrence. When the risks has been analyzed and prioritize, the author uses the elements of corporate security areas to give recommendation on how to protect the case study company assets including the safety of the customer, employees, and the valuable information.

In this thesis, the author use both quantitative and qualitative risk analysis to analyze the risk. In the quantitative analysis, the authors use the Annual Loss Expectancy (ALE) as a method to prioritize the risk. After the risk has been prioritized then risk that has the highest impact toward the company will be further analyze using bow tie analysis to find the clear image of the source of risk, preventive control, and to find the consequences of the highest impact risk for the company.

This thesis has managed to identify, prioritize and thoroughly analyze various threats that exist within the case study company. Furthermore, it provides the path and various suggestions towards the existing threats and risks that are potentially disturbing the business continuity of the company.

Keywords: Business Resilience, Risk, Risk Analysis, Annual Loss Expectancy, Bow-tie Analysis, Asset protection, Corporate Security

Table of contents

Introduction

In every business, both big and small, there will always be events which may cause business disruption and unable to be avoided completely. Thus, it is a wise option to analyze the risk and plan for it in order for the disruptions to be handled as efficiently as possible. Pre-planning is the essence of continuity and its procedures explain how to handle the situations quicker compare to the possible confusion that most likely to arise when no plans are available on how to minimize the impact and protect company assets during a business disruptions. (Hotchkiss 2010)

In most cases, critical or non-critical situations, it is beneficial to have prior knowledge of risks and prepare preventive measure to handle the situations. Enterprises are vulnerable to risks that often disturb or destroy the business operations. Therefore, it is important for the organizations to identify and plan to mitigate the possible risks and threats.

Risk analysis helps the business to identify risk and analyze it based on its impact that can potentially harm the organizations. It also supports the business to plan the measures to reduce and prevent risks so that it will not disturb the business operations and creates catastrophes. (Sandhu 2002)

As the company is growing, the need of security protections in the company also increases since there are valuable assets and information that are stored in the company. For that purpose, the authors initiated discussion with the case company representatives on how to protect their valuable assets through risk analysis to ensure business resilience. From the discussion, the author proposed the ideas to construct a risk analysis for the company in order to identify and analyze all the risks which can potentially harm the company, and able to provide the path on how to protect the assets by using corporate security.

1.1 Company in brief

The case company in this thesis study is the company that owns two speciality stores that provide Asian and African products within the Finnish and Scandinavian market. The company supplies over thousand products that range from food and beverages, daily needs, until cosmetics and accessories. Most of the market segments are within the Swedish and Finnish retail sector. With the low and competitive prices, the company has been successful in the retail industry, particularly in Finland, since its inception in 1995.

According to the manager, each shop has a weekly sale of about 14000 €. There are four employees who work every day; one key employee works throughout the whole business hours in each of the shop and two employees are in charge of delivering orders and taking products

from storage to the shop. In addition, one extra employee is hired as a helper during the weekend.

In this thesis, the author will concentrate her research only in one of the company stores. Since significant portion of the profit comes from the shop, therefore it is considered important to know what kind of risks that the store might have. Due to the security reason, the author will classify the name of the company in this thesis.

The core value of the case company is to meet the customer's demand and needs by providing high quality of special food products and cosmetics that cannot otherwise be found in local Finnish market, whilst keeping the product prices as affordable as possible. What the company provides to its customer are various brands of products as well as food and beverages, both fresh and dry, from India and many other parts of Asia as well as Africa.

In regards of valuable assets, the company's representative enlightens that currently their valuable assets are the company building, machinery, vehicles, inventory, and employees. These various valuable assets are the ones that build the foundation and objectives of this thesis. Risk analysis of these assets can possibly be the most important factor that plays role in the business continuity of the case study company.

1.2 Objectives of Study

There are three objectives of this study. First is to identify various threats, both internal and external, through risk identification to recognize potential risks that can harm the case company business operations and assets. Second is to analyze how to prioritize and find the consequences of risks using the quantitative and qualitative risk analysis, and the third is to protect the company assets including the safety of the customers and employees by implementing the corporate security areas.

The outcome of the thesis will be used by the company as a platform to raise the awareness of the risks that the case study company might face that can possibly lead to loss for the organization. Additionally, by knowing both internal and external risks, it will help the case study company to prepare what kind of security protection that is needed in the company.

1.3 Research Questions

There are several questions that the author acknowledges as a gap which will be understudied by this thesis. These are the research questions:

1. What are the various risks that might be affecting the business operations of the case study company?
2. How to prioritize and mitigate the risks?

3. How can the aspects of corporate security able to protect the business assets and functions of the case study company?

1.4 Research Approach

The main objective of the thesis is to identify various threats by analyzing the risks. To find the answer, the author uses a combination of observational, literature, quantitative and qualitative methods regarding risk analysis as research methods.

1.4.1 Theoretical framework

Figure below show the theoretical framework of the thesis and it will show three stages of the thesis writing process.

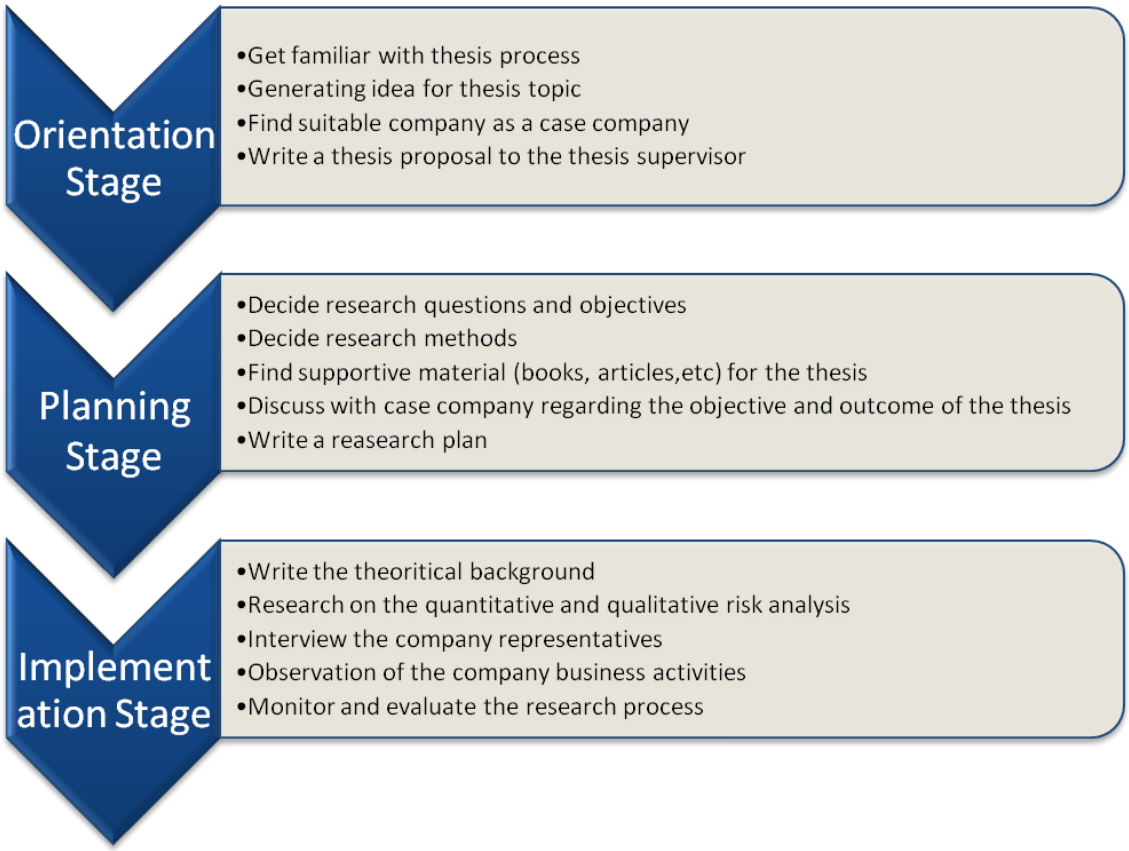

Figure 1: Theoretical framework

1.5 Thesis Framework

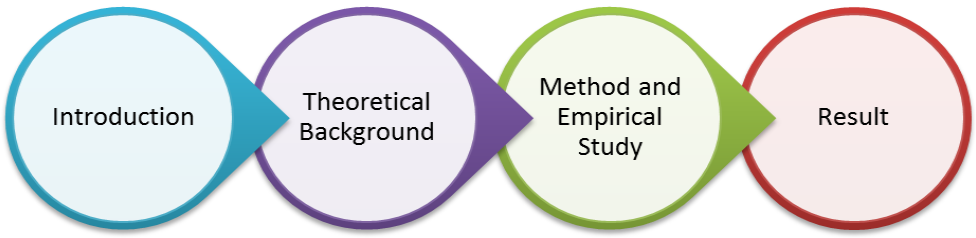

Figure 2: Framework of the thesis

This thesis consists of four chapters. The first chapter is the introduction part; it briefly explains the case company and shows the purpose of the study including research questions and its framework.

The second chapter describes the theoretical background. It starts with explaining the business resilience in order to give the reader a better understanding on why every company needs good business resilience. After that, the author will introduce risk analysis with its methodology, and how the corporate security assets are able to protect company valuable assets. The theoretical part will help the author to generate and refine the research ideas.

The third chapter explains the method that is used in the thesis and empirical study of the case company. The last chapter will give the reader information regarding the result of the thesis.

2 Theoretical Background

2.1 Business Resilience

Recent events in the world have brought risk into higher awareness. All the natural or man-made risks, like earthquake or terrorism, represent the extreme risks that are facing the society and business.

As Thoma (2014) stated in his article, resilience is the ability of a company to prevent hazard that can disturb the business operations by being well prepared to prevent the occurrence of the threats and taking appropriate measure as response to it. Business resilience is the company's ability to endure the unexpected situations and rebound from any loss that occur from the events.

The resilience system should reduce disruption probabilities and consequences, as well as time to recovery. With its ability to adapt and respond to a business disturbance, business resilience usually begins by understanding the company requirements to survive from unexpected events and plan for the unpredicted future challenges. In other words, business resilience goes one step ahead of the business continuity by offering post-disaster strategies to the company to maintain business operations during period of disruption. (Thoma 2014)

Examples of disruption on the case company store are fire, power blackout, employees get injured in the workplace, supplier could not send the product in time, etc. There are many other threats that can affect the company business operations, therefore the company are advised to identify various other risks that can harm the company. By knowing its potential risks, the company will be able to increase its business resilience by reducing the probability of the risk to occur and its impact.

There are some challenges that the company might have during the implementation of business resilience. From an IT perspective, implementing resilience requires the company to use advanced technologies, e.g. firewalls and encryption. It is also challenging to maintain the availability of business service during a disruptive event. However, if the company manages to implement the business resilience strategies effectively, it will be able to save the company's money from acquiring the unnecessary technologies by fully understanding the level of protection they need for an unfortunate event and construct a strategic plan for that purpose (Business Resilience 2009).

Cooke (2013) mentions in his article that the resilience relies on three factors:

1. Flexibility: These are the company's capability to make changes when it is necessary to effectively respond to the changes that happen in the company.
2. Adaptability : The ability to adapt to the changes and how the company can apply the changes in the business operations
3. Learning: The ability to learn from having to adapt or be flexible towards the changes to avoid the same disruption to happen again.

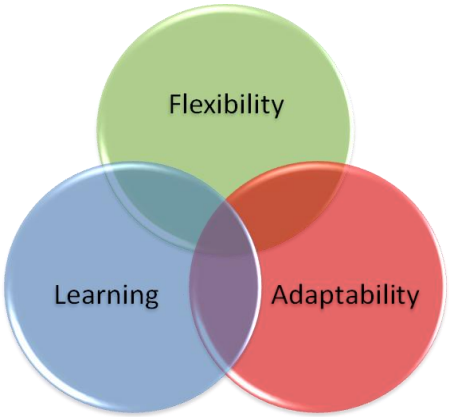

Figure 3 : The three factors for resiliency (Cooke 2013)

In general, company needs resilience in its business to bounce back when it is facing harsh conditions. Example of a good resilience company can be seen from article written by Birkinshaw (2012) in the business week websites regarding the giant automobile company, Toyota.

Back in 2009, the well-known company experienced several big crisis, starting from a problem with the car windows which resulted in a total of 7.4 million vehicle recall, to a problem with unintended car accelerations, a supply chain issues, tsunami in 2010 and eventually a 50% sales drop in their biggest market, China, due to political tensions between China and Japan.

Despite all the various problems, the way Toyota dealt with them shows a good example of resilience. During a crisis, Toyota president, Akio Toyota, gave a public statement regarding a crisis that the company face, offered an apology to the public, and admitted that Toyota has

distant itself from the customers. After the president gave a public statement, the company slowly gained their customer trust and overcame the crisis.

It can be seen from the story that the company had the ability to bounce back when facing a crisis. Good resilience can be seen by having the ability to adapt to the changing business environment, quickly response to a crisis, willing to admit and also learn from the mistakes to prevent the same problem happening in the future.

According to Thoma (2014) concept of resilience is closely related to risk that pose a threat to business continuity. Therefore in the next chapter the author will talk about risk analysis to prevent a crisis through risk classification and evaluation.

2.2 Risk

According to Sandhu (2002, 64) risk is defined as "the possibility of suffering harm or loss; danger." In other words, risk is a danger that can happen in any businesses. It is wise for the company to assess the risk's impact towards its business and create a suitable business continuity plan to maintain the continuity of its business operations.

Hopkin (2012, 14) defines risk in his book as an event that has the ability to give impact to the company's projects, strategy, operations and business processes.

From the two authors, it can be concluded that risk is anything that has the possibility to give certain impact towards the company's business process and strategy, as well as having the ability to lead the company to a harmful situations.

Sandhu (2002, 65) mentions that there are three elements of risks:

- Risk Event
  It is described as natural or man-made event that results as a potential threat.
- Risk Probability
  It is defined as probability of a risk, or threat, to happen. Normally, the data can be collected and analysed from the past events.
  According to Blyth (2009, 20) probability of risk is divided into these categories:
  - Low: The probability of risk occurring is low, and no special measure should be implemented other than standard company policies and procedures.
  - Medium: There is a chance of risk to occur, therefore those that have been categorized as medium risks will need a certain measure to mitigate the risks.
  - High: Since there is a high possibility of risk to occur, the company needs to prepare an appropriate budget to create policies and procedures to counterattack the likelihood of the risk occurring.

- Extreme: This type of risk will definitely occur at some point of the business activities. If a probability of risk occurring is extreme, then the company is recommended to accept the impact and protect the business with the detailed business continuity management plan or consider whether or not to continue its business activities.

- Risk impact
  It is defined as the loss or damage caused by a risk.

Tabel 1: Risk Elements (Sandhu 2002)

NO	Risk Event	Risk Probability	Risk Impact
1	Suicide bomber	Low	Building evacuation, injury, loss of life
2	Fire	Medium	Building evacuation, financial loss, injury
3	Computer virus	Medium	Data loss, information disclosure
4	Power blackout	High	Power surges, insufficient power to backup system, shutting down production and telecommunication

From the example of power blackout in the above table, the probability of occurrence in the case company area is high. Therefore, the presence of power generator can reduce the impact and minimize period of disruptions in the company.

2.3 Scope of Risk

According to Blyth (2009, 141), understanding the scope of risk will enable the company to have a more comprehensive knowledge about how to manage the company before, during, and after a crisis event so that the direct and associated impacts of a risk will be understood and can be prevented before it occurs.

In his article, Tyson (2010) mentioned that risk can come from outside or inside the organization. Risks that come from inside the organization can basically be categorized as internal risks. Examples of this type of risks are personnel issues like illness, unanticipated termination of key personnel, incompetence of the manager, changes in production or distribution, etc.

Threats that come from outside the organization are categorized as external risks. This type of risks is hard to predict because it comes from the outside, and oftentimes the company does not have the power to control it. An example of external risks are the problem with

transportation, key supplier going bankrupt, wars, or other events that can have a direct impact with the business operations. (Tyson 2010)

Based on Wallace (2011, 41) it is useful to separate the threat into categories in order to prioritize the risks. So when evaluating the risks, he distributes them into different layers:

1. External risk
   - Natural disasters: Floods, earthquakes, hurricanes, tornadoes, pandemics, extreme temperatures, snow storms, etc.
   - Manufactured risk: This type of risk is the result of someone else's disaster or actions that affect the company business operations. It can be a transportation disturbance, broken pipelines, chemical leaks, etc.
   - Civil risk: This event is caused by civil disturbances like riots, labour disputes, terrorism, etc
   - Supplier risk: In here, the company consider all the risks related to their suppliers.

   Risks in the external layer typically affect the customers, suppliers, and employees.
2. Facility-wide risk

   This type of risk only has an impact on the company local facility. Example of risks that fit into this category is: electricity, telephones, water, climate control (loss of heating or air conditioning), data network, fire, structural problems, security issues (workplace violence, trespassing, sabotage, theft of confidential company information), medical concerns (death, sickness, and accident), etc.
3. Data systems risk

   The main purpose of examining data systems risk is to discover the company's single point of failure. The risks in this category are related to company networks, central computer systems, internet access, and server.
4. Departmental risk

   This is disruption that might happen in the company's own department.

While according to Hopkin (2012), risks are categorized as such:

- Strategic risk: The risks in this type can be classified as risks in the business strategy, business vision and mission, or business model.
- Tactical risk: These risks are more related to the financial side of the business. It includes the liquidity and capital.
- Operational risk: These risks are in the company assets and company methods to perform the business strategy which includes people, technology and business process.
- Compliance risk: These are the risks for a company earnings or capital by not following the regulations and laws. Fines, compensation of damage, or invalid contract are the results if the company fail to obey the necessary standards.

There are many other types of classification. The company can use the above mentioned method, a combination of these, or an entirely new classification. For instance, the company can simply classify the risk into man-made and natural risks or critical and non-critical risks. However, the purpose of risk classification will remain the same, which is helping the company to prioritize and focus towards the risks that have big negative impact so that the company can have certain preventive measures to mitigate them.

2.4 Risk Analysis

As mentioned earlier in chapter 1, the concept of resilience is closely related to risks that can affect the company business operations. In risk analysis, the company will identify and categorize all the risks that can potentially disturb the business operations. By analysing the risk, it can be one of the ways for the company to increase its business resilience as it will be able to predict the risks and prevent the occurrence of every possible risk.

Risk analysis helps the businesses to prepare themselves from all the risks that might disturb their operation by analysing the threats from its frequency of occurrence and the impact toward the company, and afterwards prepare the necessary action to mitigate them.

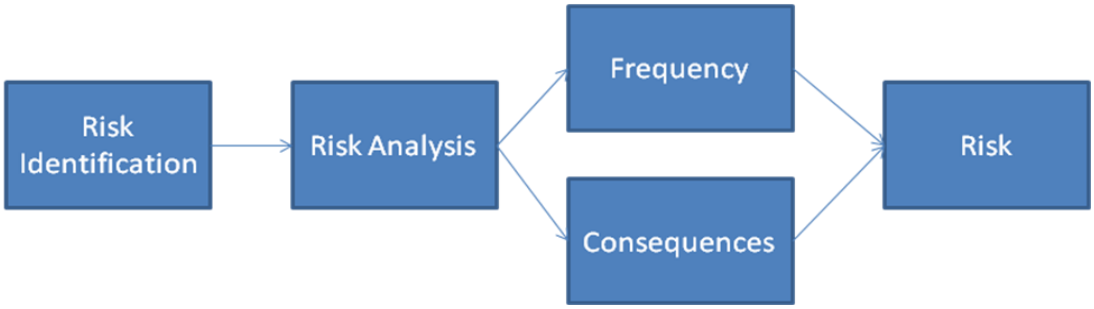

Figure 4 : Risk Analysis phases (Sandhu 2002)

The process of risk analysis involves defining and analyzing risks that can harm the business operations. In other words, risk analysis can also be concluded into four steps using a simple abbreviation of IERR:

- Identify and measure the level of the risk
- Evaluate the risks
- Record the risk to risk register
- Respond the risk (Sterling et al. 2012, 75)

By using the IERR process, the company can evaluate how risks can give influence to the business. For example when the company tries to identify business' risks, it needs to consider not only its organization, but also the risk environments. Therefore, according to Sterling et al. (2012), they divide the risk environment into three areas (see figure 4).

Wider environment includes, e.g. transportation disruption where the company has little control for the risk, immediate environment where the company has more control over, e.g. contract with suppliers or distributor, and internal business environment where it happens inside the business and the company can control the risk.

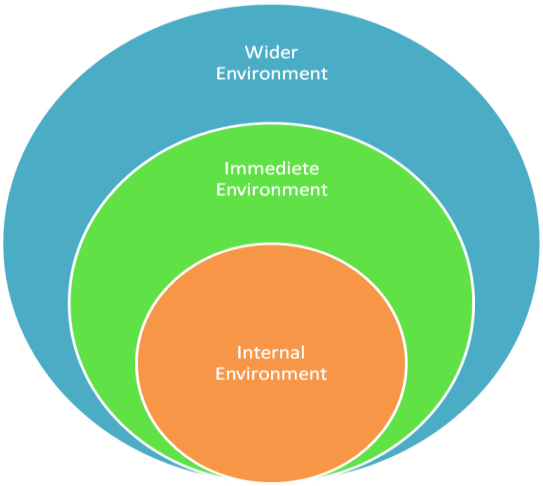

Figure 5 : The risk environment (Sterling et al. 2012)

An event must occur in order for a risk to happen. For example, consider what could disturb an outdoor concert. The events that can cause disruption in a concert may include a power blackout, rain, delay on logistic, accident near a concert place that delays the arrival of the audience, the absence of a band members, etc. Having identified all the events that can disturb the performance, the management can then decide what step they need to take to reduce the chances of one of the above mentioned events from happening. The analysis that is done by the management of the concert is an example of risk management.

According to Thomas (2014), risk matrixes are used to provide overview of all risks that can disturb the company operations. A risk matrix classifies risks based on the impact and probability of occurrence.

The risk analysis can be used as a recommendation for establishing an effective security program to protect the company business operations. For instance, if the risk is identified as the one with minimum or low impact, the company can simply ignore it. However, if the risk has been categorized as a high impact, then the company needs to allocate a budget to implement immediate security measures and set an effective security protections program.

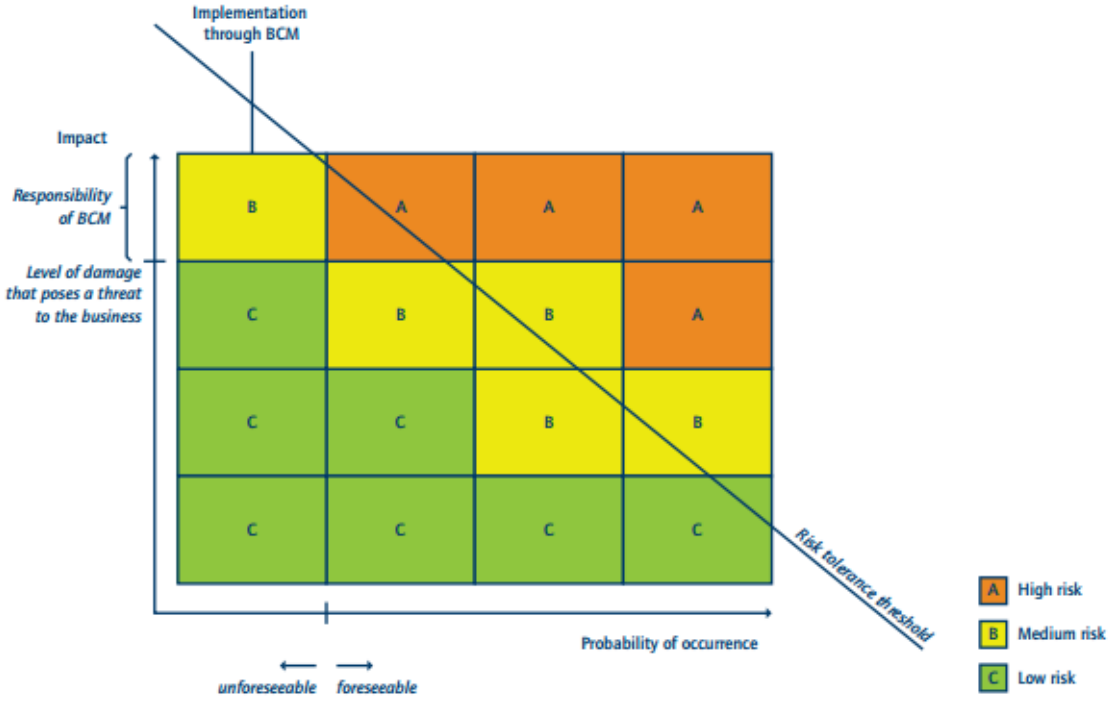

Figure 6: Risk Matrix (Thoma 2014)

There are many various advantages that the company can get by analysing the possible risk that might disturb the company business operations. Risk analysis plays an important role to identify and prioritize critical activities and functions inside the company. Not only that, it is also able to identify risks that are likely to harm the company and check whether the company is ready to protect itself from the identified risk. (Sandhu 2002)

In addition to that, the method of risk analysis provides a path for the employee to learn more about risks that might occur in the daily activities. This will help the employee to avoid the risks that are caused by employee negligence, and furthermore, they might also help to identify new risks that have not been discovered. (Sandhu 2002)

2.5 Risk Analysis Methodology

Risk analysis is a crucial part in security assessment since it calculates and determines the frequency of disruption events and the impact of their occurrences. There are two ways that can be used to calculate risks. The company can use the method to compare the damage that is caused by a risk with the cost of the measures to reduce the impact of the risk.

According to Sandhu (2002, 71) the methodologies to measure risks are:

- Quantitative risk analysis
- Qualitative risk analysis

The author will explain more about the methodologies in below sections.

2.5.1 Quantitative risk analysis

In the quantitative analysis, the risks are measured using the monetary terms and figures. In this method, the risks are considered as a cost to the company. The company can then calculate the exposure to risks and the annual loss expectancy (ALE). (Sandhu 2002, 72)

Quantitative risk analysis determines the level of risk from an event. Normally, it can be determined by using two values: frequency and impact. The function of the two values is known as expected values (EV). However, as time goes, the method is expanding and companies are more interested on using the annual loss expectancy (ALE) method to evaluate the risk. The company can plan its budget for risk management by using the ALE methods. (Elliott et al. 2001, 129)

At the beginning, ALE was intended to evaluate the information technology risks. However, due to its benefit of calculating the cost of every risks, now it has become one of the methods that can be used for quantitative risk analysis. The ALE method is an extension of the EV approach. ALE is defined as the loss likely to be caused in a year by a risk. (Elliott et al. 2001, 129)

The formula to calculate ALE is developed by calculating the frequency of occurrence (f) and the impact (i).

Impact (i)	
10 €	let i =1
100 €	let i =2
1.000 €	let i =3
10.000 €	let i =4
100.000 €	let i =5
1.000.000 €	let i =6
10.000.000 €	let i =7
100.000.000 €	let i =8

Frequency of occurences (f)	
Once in 300 years	let f = 1
Once in 30 years	let f = 2
Once in 3 years	let f = 3
Once in 100 days	let f = 4
Once in 10 days	let f = 5
Once in 1 days	let f = 6
10 times per day	let f = 7
100 times per day	let f = 8

Figure 7: Calculation of ALE (Sandhu 2002, 132)

For example, by using the formula, it can be seen that a risk that occurs once in 3 years and creates loss of 10000€ for every occurrence will have an annual loss expectancy of 3333€.

$$\text{Impact rating: } \frac{10^{(f+i-3)}}{3} \qquad \text{Impact rating: } \frac{10^{(3+4-3)}}{3} = 333{,}333€$$

The author uses ALE in a quantitative analysis due to its ability to analyse the risks probability and the impact. As mentioned earlier by Elliott et al (2001), the ALE calculates the impact of risks to identify the risks that are likely to cause the maximum loss. By knowing the cost for every risk, it will help the company to assess and compare the potential financial impact of a risk with the cost of implementing measures to mitigate the risk. Based on the potential impact of a risk, the company can allocate appropriate funds toward its mitigation.

ALE is a useful method in evaluating the cost effectiveness of a security measures to mitigate the risk. However, the data can be unreliable and inaccurate since the company is unlikely to be able to measure the probability of all risks. In addition, up to this moment, there is yet a standard formula to calculate the risks using ALE method. Consequently, when it is not possible to calculate risk quantitatively, then the company needs to use qualitative risk analysis.

2.5.2 Qualitative risk analysis

The company mostly uses the qualitative analysis when it is not possible to calculate the risk accurately. When evaluating the risks using this method, the company needs to consider factors such as landscape of the area, geography, and proximity to highway that transport dangerous material. (Sandhu 2002, 75)

Qualitative analysis generally classifies the risks into low, medium, and high. The analysis is usually gathered from an interview, company's history, test, and personal experience of the person doing the assessment. (Kovacich & Halibozek 2003, 39)

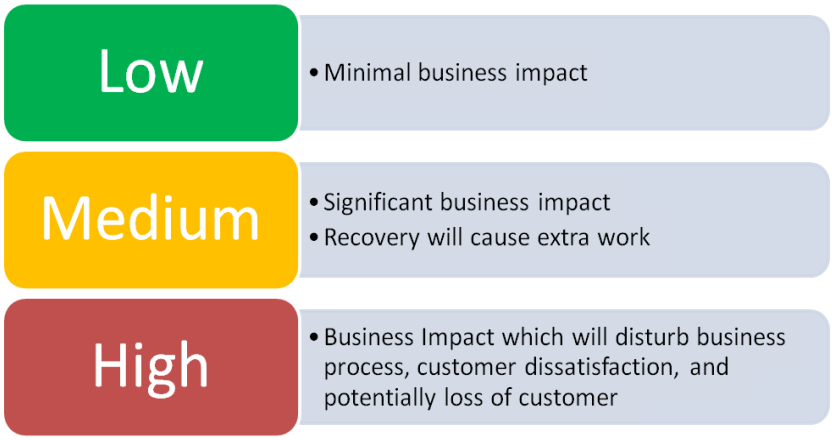

Figure 8 : Qualitative analysis method (Hotchkiss 2010)

When a risk is categorized as a high risk, the company is advised to take prompt action to reduce it. For a risk that is classified as medium, the company requests to take suitable measure to mitigate it. And for the low risk, the company can disregard it since it will not disturb the company business operations.

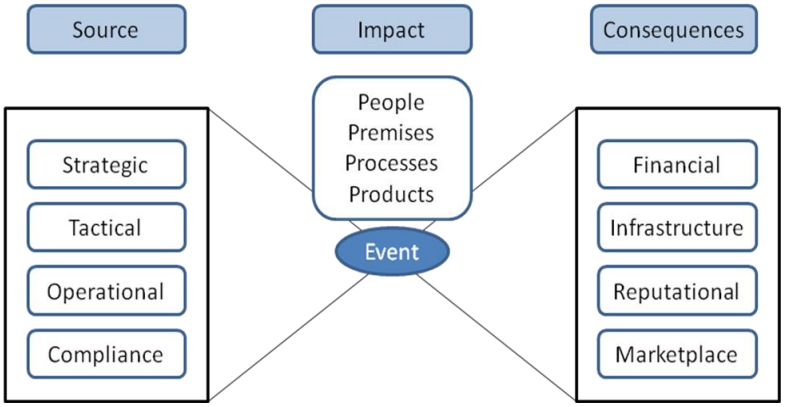

Figure 9 : Risk Management and bow-tie (Hopkin 2012, 47)

In a qualitative risk analysis, the most popular method to use in analysing risks is by using a Bow-tie diagram (See figure 7). A bow-tie is an easy way to understand a risk analysis. The purpose of the bow tie illustration is to demonstrate and clearly displays the connection between the source of risk, preventive and response controls and impact of an accident. (Hopkin 2012, 48)

However, this method is lack of efficiency. If the company wants to analyze the risks then it needs to analyze the risk one by one according to the event. So in that case, if the company is vulnerable and has quite many risks, then it is not advisable to use this method as they need to analyze each one of the risks.

The author chooses the bow-tie as qualitative analysis to analyse the case company because it is suitable for the case company type of business. Since the case company store is relatively small, each threat can still be analysed by using this method. Bow tie analysis can be a good method to communicate risk issues to person who is not a risk specialist as it provides an easily-understood visualisation of the relationship between the source, impact and consequences of a risk.

From the diagram, the centre of the bow-tie is the risk event. The left-hand side of the bow tie represents the cause of a particular event. In figure 7, the source of a risk can be from a strategic risk, tactical, operational, and compliance risk. While on the right-hand side of the bow-tie explains the consequences of every threats when it occurs with the possibility of disturbing company financial, infrastructure, reputational or marketplace.

Example of bow-tie diagram can be seen from the figure 8.

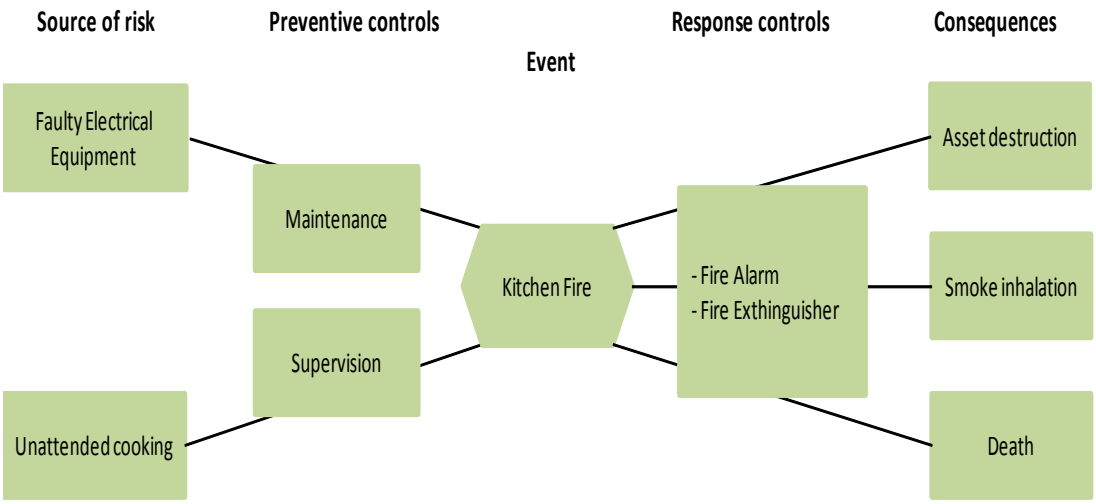

Figure 10 : Bow-tie diagram (Hopkin 2012, 48)

2.6 Assets Identification

As mentioned earlier in this thesis, the risk analysis is useful to minimize the impact and protect company assets during business disruptions. Therefore in this section, the author will identify various assets that are important and valuable for business.

According to Hopkin (2012, 79), any resources that are important for business to maintain its operation can be defined as an asset. Norman (2010, 47) mentions that all organizations have four types of assets:

1. People (Employees, Customers, Visitors, Management, Vendors, etc)
2. Property (Equipment, Building, Vehicles, Furniture, etc)
3. Proprietary Information (Security System, Strategic Plans, Customer lists, Accounting records, Vital records, Research Plan, etc)
4. Business Reputation

In order to protect the assets, it is important for the company to know what its assets are and the consequences if it is not able to protect the assets during a period of disruption.

2.7 Asset Protection through corporate security areas

According to Kovacich (2003) “the corporate security is the security function owned by and operated within a business”. The concern of this function is to oversee and manage the safety of all business functions and assets. This can cover from the basic loss-prevention activities and compliance to business continuity planning.

Diagram below shows the area of corporate security according to Confederation of finnish Industries (Elinkeinoelämän keskusliitto(EK))

Figure 11: Corporate Security Areas (Yritysturvallisuus)

Tabel 2: corporate security area (Yritysturvallisuus).

Areas	Objectives	Key contents
Production and Operation Safety	The purpose of this section is to have a safe process from a raw material, labour, and energy to products or services. It also involves the responsibility to make sure the operation is effective and efficient.	- Risk assessment and contingency planning - Product liability and safety at work - Service safety - Logistic safety - Information security agreement - Sub-contractor and service provider
Occupational health and safety	The objective of this area is to promote health and safety in a workplace. It protects the employee, family member, customer and others who might be affected by the workplace environment.	- Employer and employee responsibilities regarding health and safety - Machinery and equipment safety - Safety in the workplace - Handling of dangerous goods - Work violence - Well-being
Environmental	To provide an environ-	- Sustainable development

safety	mental protections	- Waste management - Chemical control - Noise protection - Water and soil protection - Air pollution and emission trading - Dangerous good handling and storage
Rescue Operations	These are the company security plan that covers the rescue plan during a fire or other disruptive situations. The objective of this area is to have a fast and correct response to an incident.	- Rescue plan - Fire safety - Safety equipment - Periodic inspection of the rescue equipment and maintenance schedule - Major incident preparations (Fire, Chemical, gas, etc)
Contingency Planning	The purpose of this area is to enable the company to maintain continuity of their business.	- Preparation for unexpected situations - Procedures to protect employees, core business elements, information systems, environment during business disruptions.
Information Security	It protects the company information from threats by protecting the confidentiality, integrity and availability of information to ensure business continuity and minimize business damage.	- Classification of information - Security clearances - Data protection - IT security (software and hardware security)
Personnel Security	Through this area, the company able to protect their workers against crime and accidents.	- Pre-employment checks - Business travel Safety - Safety of the customers - Security education and awareness training for the employee - Enterprise personal safety - Termination of employment - Changes in work roles

Physical Security	This is the fundamental aspect of protection. This area uses the physical controls to protect company premises, facility, building, site, or other physical assets belong to the company from any loss or harm. Physical security is also able to protect the employee and information stored in the building.	- External barriers : Doors, Fences, walls, gates, buildings, surveillance camera, Lighting, alarms, etc - Internal barriers : Control systems
Security of International Operations	The objectives of this area are to ensure personnel safety is guaranteed when the employee is travelling abroad.	- Risk assessment of designate country and analyze how the work task will expose the employee to risks. - Create policy and procedures for travelling abroad - Train the employee regarding travel dangers and how to act during an emergency situations abroad
Crime Prevention	The purpose of this area is to reduce and prevent crime and criminal. The measure focus on company operations, personnel, and assets.	- Train employee regarding crime prevention - Cooperation with authorities - Criminal risk management measures - Create policy and procedures regarding criminal activities.

2.8 Risk controls

There are several ways that can be used to control risks. According to Hopkin (2012, 236) “the most convenient classification system is to describe these controls as preventive, corrective, directive, and detective.”

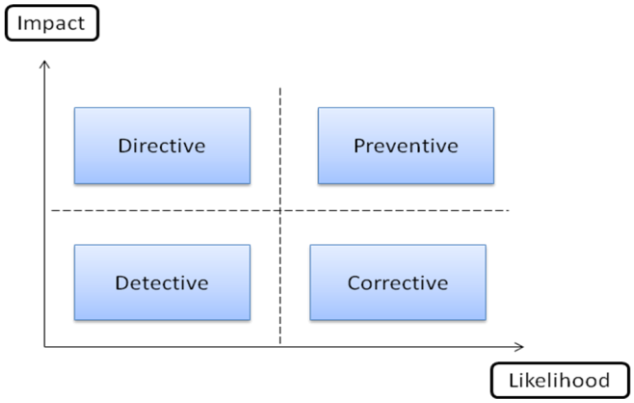

Figure 12 : Types of risk controls (Hopkin 2012)

The preventive control is designed to limit the probability of a risk to occur. Example of preventive control is by having pre-employment screening of potential staffs or removal of the source of dangerous material from workplace, limits of authorization, policy and standards, etc. (Hopkin 2012)

Corrective control is created to limit the scope for damage and reduce unwanted outcomes that have been materialized. This type of control is also designed to correct the situation by restoring the system or process back to normal situations. Examples of this control are passwords or other access control, staff and job rotation, or limitation of working hours. However, the restoration process may create loss for the company since it may lead to customer dissatisfaction, unavailability of products or services, and many more. (Hopkin 2012)

Directive control is designed to guarantee that a particular result is achieved; it includes providing direction to employee to make sure that losses do not happen. For example, a directive control would cover detail instruction for the employee to follow and employee training on how to respond during a particular risk events.

Detective control is designed to identify errors after they have occurred. Examples of the control are reconciliation, audit, and review of performances. This control is intended to detect when the unwanted situation have happened to ensure that the conditions do not get worse further. (Hopkin 2012)

Of these four types of controls, preventive control is surely the most effective since it is able to minimize the possibility of damage by preventing the event from happening, followed by the corrective and directive controls, since they can minimize the impact of the loss by restoring the system. The least effective control is the detective since it identifies an event after it occurred.

3 Method and Empirical Study

3.1 Limitation of the thesis

The information that is contained within this thesis is based on reliable sources of company website, interviews and direct observation. However, due to security reason, the results of this thesis will be limited in terms of risks analysis. Hence, risks that are considered sensitive information for the case study company will not be mentioned or made public.

3.2 Case company business resilience

As it mentions in chapter 2, business resilience able to reduce the probability and consequences of a disruption, as well as time to recover from the disturbance. Therefore it is important to the case company to implement business resilience in their business operations. As it is the ability of the company to overcome the crisis by adapting to the changing business operations, quickly response to the crisis, and learn the mistakes to prevent the disruption to happen again in the future.

As mentioned by Cooke (2013), there are three foundations in business resilience. The importance of the business resilience is applicable to any industries, including the case study company. According to the manager of the store, by implementing the three factor of business resilience it can help the company to recover when it is facing harsh conditions. For example when there are problem with the freezer, by implementing one of the factor of resilience, flexibility; the company will directly remove all the frozen goods to other freezer or directly bring the frozen items back to the cold storage before the products inside the freezer is melting and cannot be sold anymore.

This study will explore the option of concrete proposals that can enhance the business resilience of the case study company.

- By doing the bow-tie analysis, the case study company will be able to come up with various prevention measures to prepare for a disruption
- The other benefit of bow-tie is the ability to come up with certain strategy to implement in order for the case study company to reduce loss. By exploring the source of risks and the preventive measurement for each of them, the case study company can relate to those that have the biggest effect in profit loss, and come up with a strategic plan to avoid or prevent them.
- In terms of risk analysis, the in-depth risk analysis method will also be implemented in this chapter in order to improve the business resilience of the case study company. The implementation will come in form of both internal and external threat

The three concepts above will be explored, analysed and implemented in this thesis. After the analysis, the results will come up as concrete proposed measurements that can be implemented by the management to be able to enhance its business resilience.

3.3 Risk Identification of the case company

As stated earlier, the first step to analyze the risk is to identify various risks that the company might have, both internal and external. Therefore, in this section, the author will try to identify various risks that might occur in the company.

To identify the risks, the author uses observation and interview as a method to obtain information regarding various external and internal threats for the thesis. The method of observation in this thesis is done through work experience. The author will then examine and analyze various risks that are taking place within the case study company. The risks will be categorized as an external and internal factor. The observation will take into consideration factors such as daily practice, weekly activities within the shop, typical problems occurring and all the relevant parties that are involved.

Based on the observation, risks that the company might have:
External risks:

- Natural Disaster: Extreme temperatures and snow storm
- Civil disturbance: Strike done by the transportation union
- Supplier issues: Product defect, transportation disturbance, price fluctuation, supply problem
- Flu pandemic
- The decrease of purchasing power due to the economic recession that could cause a slowdown in customer spending
- Finnish regulations regarding food safety, product selections or limitation of opening and/or selling hours
- Price competition
- Changes in supply and demand

Internal risks:

- Shoplifting
- Fire
- Customer harassment to the shop employee
- Vandalism of company property
- Power failure
- Outsiders identify the door security code
- Loss of heating or air conditioning
- Freezers and refrigerators problem

- Internet access disturbance
- Staff injury
- Products are given free to the employee's friends and family
- Staff member stealing products
- The cashier employee keep the payment money for themselves
- Employee commits act of misconduct against the customer
- Loss of important staff
- Intentional destruction of important document

To get an additional support of the data, the interview was done with the company's general manager. It was conducted in a company office and the questions asked were related to the company's assets and risks and also the corporate security of the company. According to the manager, various risks that they have are:

- Shoplifting
- Vandalism of company property
- Problem with the server
- Staff injury
- Flu pandemic
- Loss of important staff
- Product defect
- Decrease of purchasing power due to economic recession
- Problem with the freezer
- Strict regulations from the Finnish authorities
- Employee lost the store key
- Fire

After identifying possible external and internal risks, the next step for the risk analysis is to analyze them. In this thesis, the author will use both quantitative and qualitative risk analysis. The quantitative will give result on which risks that the company needs to prioritize based on the calculation result between the impact and frequency of occurrence. After the prioritization has been done, the author then uses the quantitative by applying the bow-tie method to analyze the highest risk to clearly display the connection between the source of risk, preventive and response controls and consequences of the risk.

3.4 Quantitative risk analysis in case company

As mentioned earlier, in the quantitative analysis, the author applies the Annual Loss Expectancy (ALE) as a method to calculate how much the risk will cost for the company if it occurs. The result of this method will provide the information for the company regarding which risks

the company needs to prioritize and the result can serve as a good recommendation to establish procedure or guidance to prevent the risk from happening.

Information regarding the impact and frequency of occurrence is gathered from the interview with the manager of the store. The author explains various external and internal risks that the company has and requests the manager to answer the frequency of occurrence of every risk together with its impact.

Formula to calculate the risk is:

Impact (i)	
10 €	let i =1
100 €	let i =2
1.000 €	let i =3
10.000 €	let i =4
100.000 €	let i =5
1.000.000 €	let i =6
10.000.000 €	let i =7
100.000.000 €	let i =8

Frequency of occurences (f)	
Once in 300 years	let f = 1
Once in 30 years	let f = 2
Once in 3 years	let f = 3
Once in 100 days	let f = 4
Once in 10 days	let f = 5
Once in 1 days	let f = 6
10 times per day	let f = 7
100 times per day	let f = 8

Impact rating formula : $\frac{10^{(f+i-3)}}{3}$

Table 3: Comparative Annual Loss Expectancy of the external risks:

External Threat for the company	*Impact value (i)*	*Frequency of occurrence (f)*	*ALE (€)*	*Priority tier*
Extreme temperatures and Snow storm	3	3	333	2
Strike done by the transportation union	3	3	333	2
Product defect	4	3	3333	1
Supplier increase the price	4	4	3333	1
Flu pandemic	2	4	333	2

The decrease of purchasing power	4	3	3333	1
Price competition	3	4	3333	1

Table 4: Comparative Annual Loss Expectancy of the internal risks:

Internal Threat for the company	*Impact value (i)*	*Frequency of occur-rence (f)*	*ALE*	*Priority tier*
Shoplifting	1	6	3333	1
Fire	5	2	3333	1
Vandalism of company property	3	3	333	2
Power failure	3	3	333	2
Outsiders identify the security door code	4	2	333	2
Loss of heating or air conditioning	3	3	333	2
Problem with freezers and refrigera-tors	3	4	3333	1
Internet access disturbance	2	4	333	2
Staff injury	2	5	3333	1
Products are given free to the em-ployee's friends and family	2	3	33	3
Staff member stealing products	2	3	33	3
Cashier keep the payment money from customer for themselves	2	3	33	3
Employee commits act of misconduct against the customer	2	4	333	2

Loss of important staff	3	3	333	2
Intentional destruction of important document	3	3	333	2

It can be seen from the table, risk that are related to personnel is very low. According to the manager, this situation happens because the management tries to maintain good and honest relationship between employee and the management. However, even though the risk is small, they understand that this situation is still a risk they need to be aware of.

From the table, it can be concluded that the company needs to pay more attention to certain external and internal risks since it will create huge difficulty for the company when it occurs.

The top highest external and internal risks are:

- External risks:
  - Product defect
  - Supplier increase the price
  - The decrease of purchasing power
  - Price competition

- Internal risks:
  - Staff injury
  - Problem with freezers and refrigerators
  - Shoplifting
  - Fire

Based on ALE calculation, it can be distinguished that there are certain risks which the company needs to prepare when it occurs since they can give immense impact in terms of funds for the company. Therefore the threats will be analyzed further using qualitative analysis.

3.5 Qualitative risk analysis in case company

From the information above, it is clear that the company needs a certain method to analyze the risks in deep to find the source of risks and consequences for the company. Therefore, in this chapter, the author use bow – tie analysis to provide practical application of the method to the identification of preventive and response control related to the risks.

However, in this thesis the author will only analyze the top highest risks, both internal and external, as the risks carry big impact for the company for every occurrence. The information that is stored in the diagram is based on the author's observations and interview with the store manager. Additionally, to differentiate between the internal and external threats, dif-

ferent colour is used for that purpose. Orange diagram will show bow-tie analysis for the external threats, and the blue diagram for the internal threats.

- Product defects:

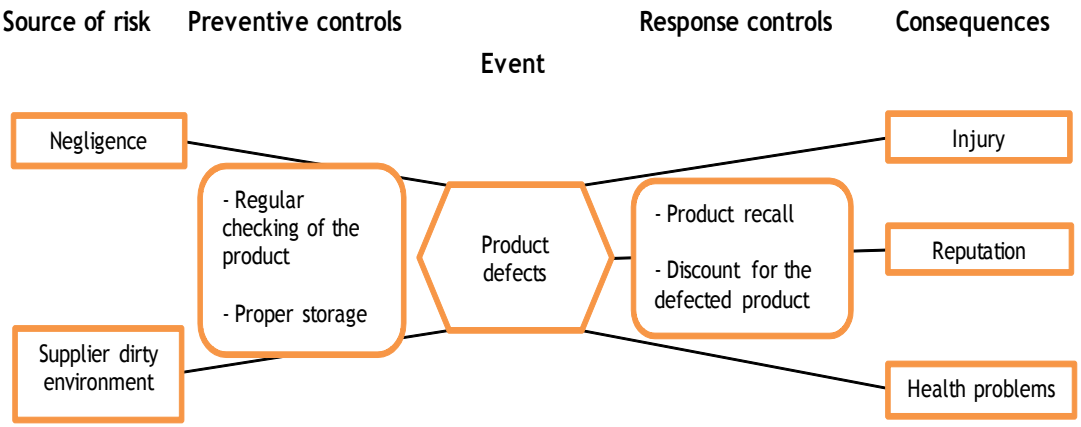

Figure 13: Bow-tie (Product defects)

- Supplier increase the price:

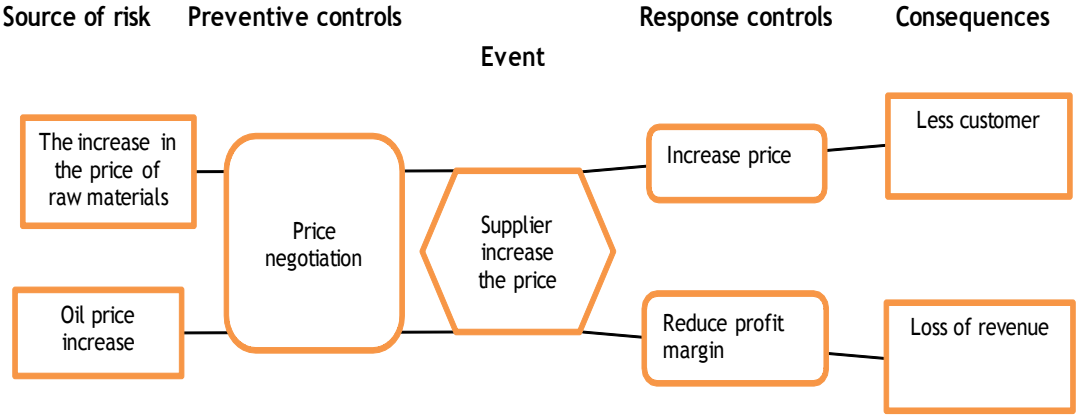

Figure 14: Bow-tie (Supplier increase the price)

- Decrease of purchasing power:

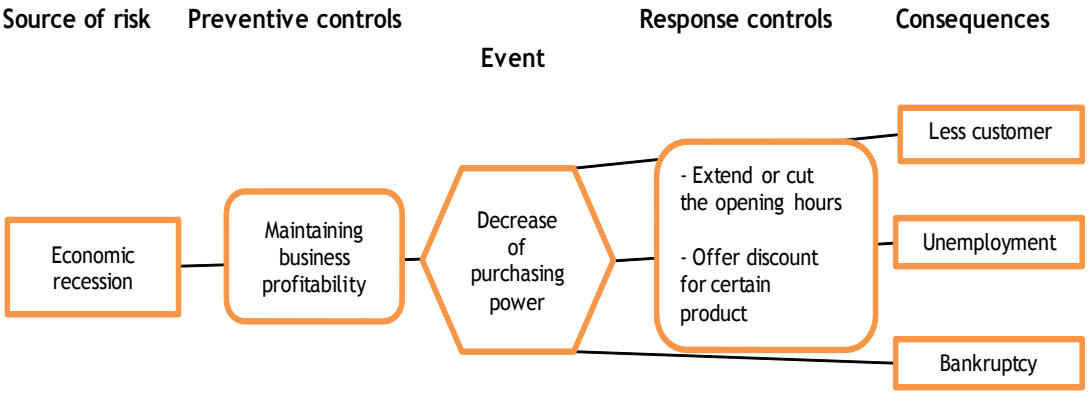

Figure 15: Bow-tie (Decrease of purchasing power)

- Price competition:

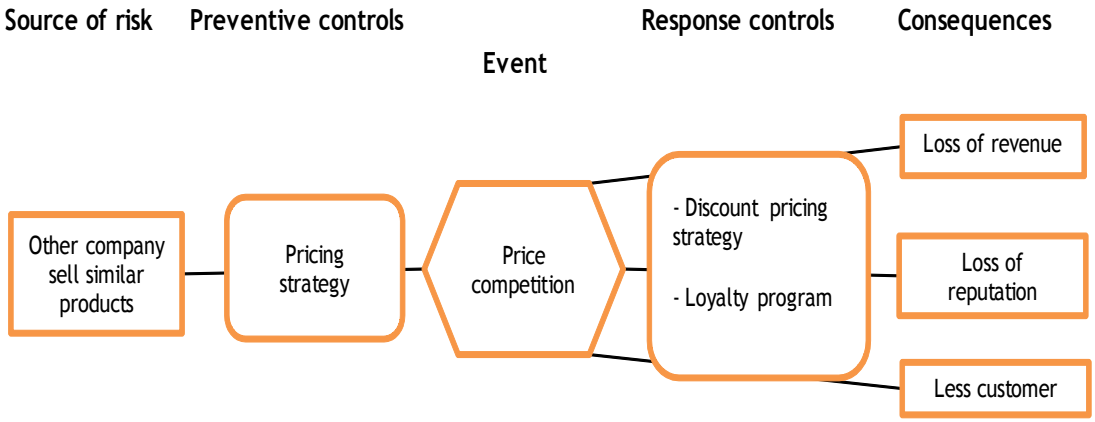

Figure 16: Bow-tie (Price competition)

- Staff injury

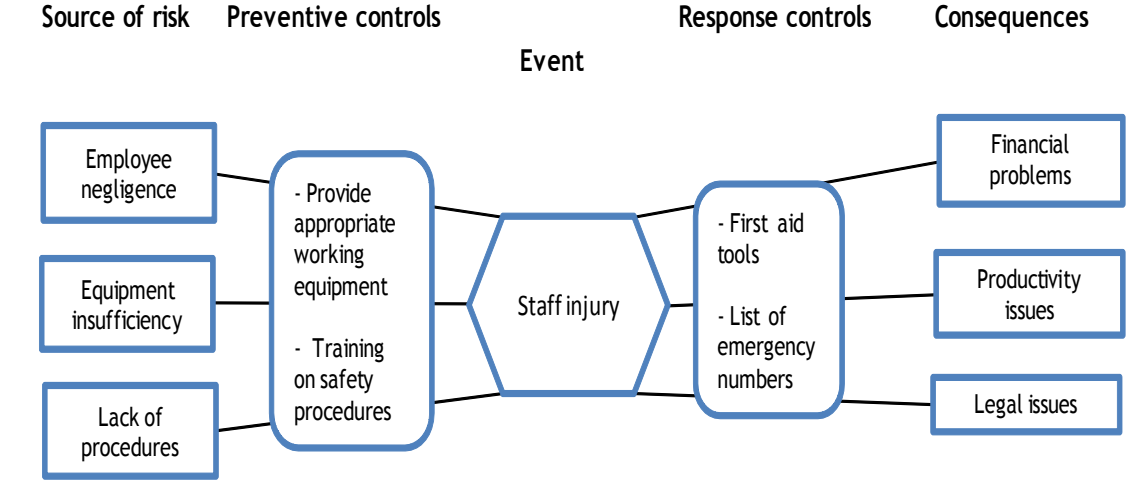

Figure 17: Bow-tie (Staff injury)

- Problem with freezers and refrigerators

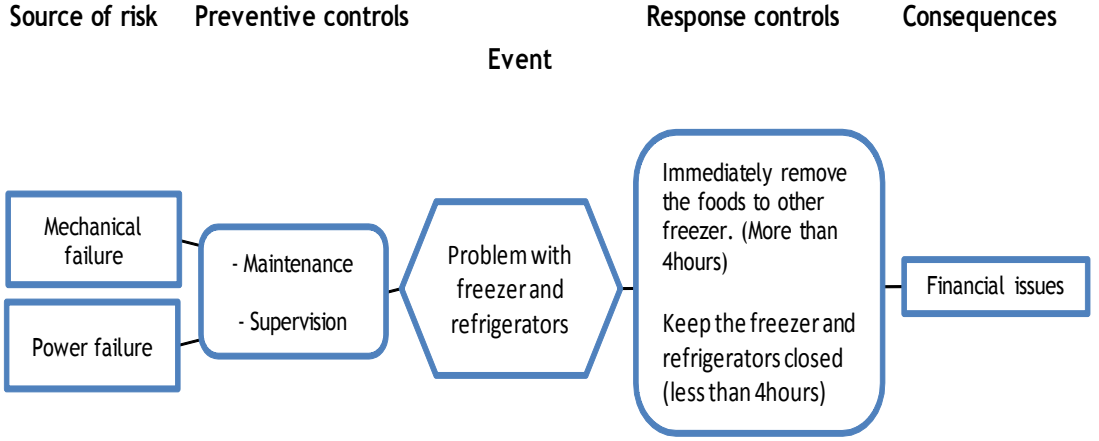

Figure 18: Bow-tie (Problem with freezer and refrigerators)

- Shoplifting

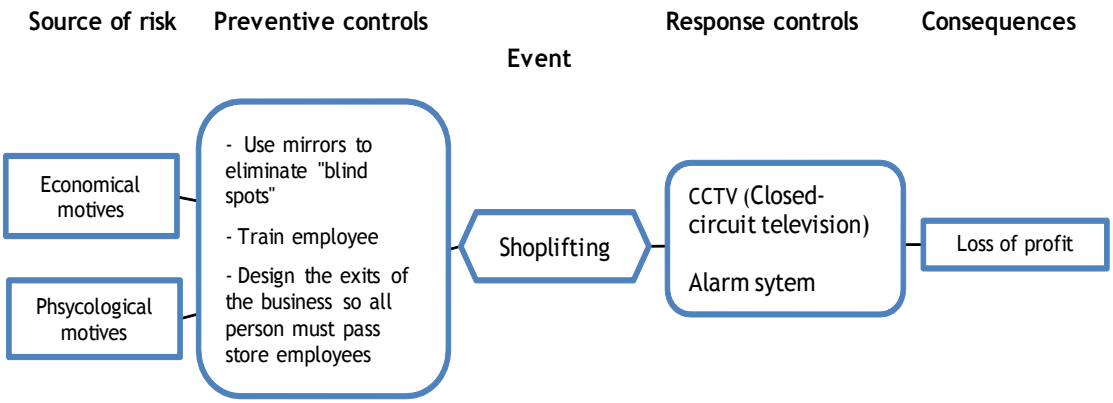

Figure 19: Bow-tie (Shoplifting)

- Fire

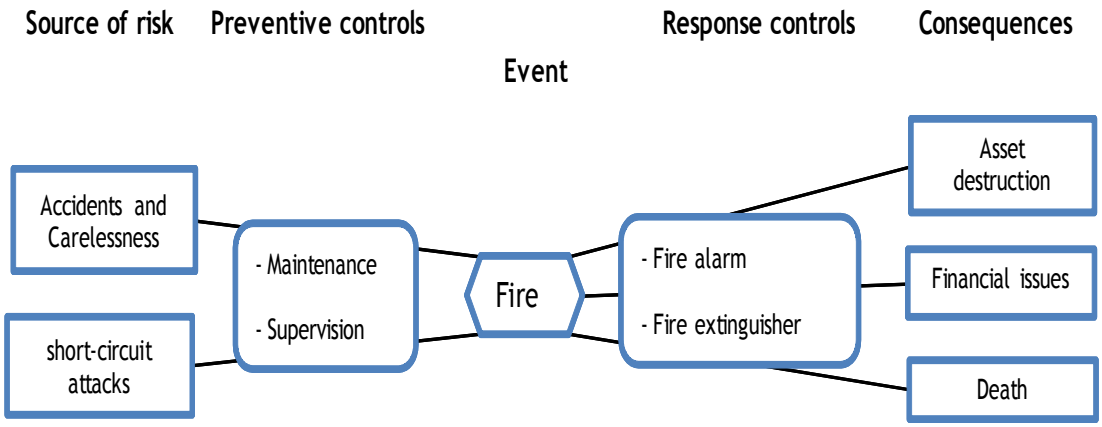

Figure 20: Bow-tie (Fire)

Bow tie analysis is a good method to find out the sources and consequences of a risk since the method gives clear relation between the event, source of risk, and result of every event towards the company. However, as mentioned earlier in chapter 2, this method is lack of efficiency. If the company wants to analyze the risks, then it should analyze them one by one according to the event. Of course, it will take time to have a complete analysis regarding various risks that the company has. The advantage of this method is that every risk is analyzed, and that the analysis results will be nearly accurate.

In addition to that, the methods of both quantitative and qualitative risk analysis will provide a path for the management and employee to learn more about risks that might happen to the company. During the risk analysis, it is recommended that the management involves the employees during the process so they can get an additional input of the kind of risks that the company might have and it will facilitate the employee the knowledge to avoid the risks that are due to employee negligence.

By involving the employees during the process could also be beneficial since the employees might help to identify new risks that have not been previously discovered based on their experience.

3.6 Asset protection through corporate security

Through risk analysis, the company is able to recognize various risks that it has. But unfortunately, knowing different risks is not enough to protect the case study company's asset if the company does not establish a procedure or method to overcome the risks. Therefore in this chapter, the author will analyze the company through the corporate security areas referred by the Confederation of Finnish Industries (Elinkeinoelämän keskusliitto).

In this section, the author will analyze the current situation of the company based on the observation and interview done in the company. According to appendix 2, the corporate security areas are divided into several points. Each of those can be analysed in terms of its implementation to the case study company.

Based on the observation done in the company, the author is able to gather information regarding the current security situations in the case company. From the appendix 2, Corporate security of the case company; The author shows which corporate security areas that the case study have managed to implement, and which ones are still yet to be developed.

As can be seen from the appendix 2, there are ten corporate security areas that can be used by the case company to protect the corporate assets: Production and Operation Safety, Occupational health and safety, Environmental safety, Rescue Operations, Contingency Planning, Information Security, Personnel Security, Physical Security, Security of International Operations, and Crime Prevention.

At the moment, there are many areas of the corporate security that the company need to develop. Examples below are taken as one of the development in appendix 2.

- Operation safety: Employee training in basic food safety, including training on hygiene practice, proper temperature control, handling expired products and food handling.

- Occupational health and safety: Provide appropriate working equipment. For example, gloves for the employees when handling frozen/fresh items and provide the first aid kit tools in the store.

- Environmental safety: Create procedure or guidelines to sort the waste.

- Rescue Operations: Create a security plan that covers the rescue plan during disruptive events and installation of safety equipment (fire alarm, smoke detectors or fire sprinklers).

- Contingency Planning: Development of business contingency program that covers emergency response, crisis management, and business continuity to decrease the probability of confusion as employees have been informed and rehearsed as to what actions to take during emergency situations.

- Information Security: Classify the information based on the level of confidentiality and establish access control to prevent unauthorised person to access the data.

- Personnel Security: Development of policy on threats or acts of violence and Pre-employment background check to reduce the chance of hiring potentially violent and criminals.

- Physical Security: Installation extra physical security for example surveillance camera, and adequate lighting.

- Security of International Operations: Create policy and procedures for travelling abroad and train the employee regarding travel dangers and how to act during an emergency situation abroad.

- Crime Prevention: Installation surveillance camera to cover blind spot area and alarm systems

4 Results

Based on both method of analytical observation and interview, various threats and risks can be identified in the company which makes the company vulnerable to disruption of its business. There are threats that are coming from both inside and outside the organizations. Example of risks that come from outside in which the company has no control over are: extreme temperatures and snow storm, strike by the transportation union, products defect, price increase by supplier, flu pandemic, the decrease of purchasing power due to the economic recession, strict Finnish regulations regarding food safety, and pricing pressure from surrounding competitors.

On the other hand, the possible company's disturbances that come from within the company are: shoplifting, fire, customer harassed the shop employee, vandalism of company property, power failure, outsiders identify the security door code, loss of heating or air conditioning, problem with freezers and refrigerators, internet access disturbance, staff injury due to various factors, e.g. lack of proper working equipments, products are given free to family and

friends by the employee, staff member stealing products, cashier keep the payment money from customer for themselves, employee commits act of misconduct against the customer, loss of important staff and intentional destruction of important document.

After the risks have been analyzed, the method of this thesis that are used to prioritize those identified risks is through quantitative analysis. By using the Annual Loss Expectancy (ALE) the author is able to calculate how much the risk will cost for the company for every occurrence and the result of this method provides the information for the company regarding which risks the company needs to prioritize. The analysis result can serve as a good recommendation to establish procedure or guidance to prevent the risk from happening.

Based on the quantitative analysis, it can be seen that: product defect, supplier increases the price, the decrease of purchasing power, price competition, staff get injured in work place, problem with freezers and refrigerators, shoplifting and fire are the top highest risk for the company.

From the information above, it is clear that those risks are the top highest risks that the company has and will creates loss or disruption for every occurrences, therefore the author use further analysis of bow-tie method to investigate the risks more comprehensively to find the source of risks and consequences for the company as well as the preventive and response control related to the risks.

By using the bow-tie analysis, every risk is analyzed carefully to get the information regarding the source of risks and its impact towards the company. For example, staff injury. Normally the cause of staff injury are employee negligence, lack of procedures or lack of protective equipment, therefore one of the example of the preventive controls are training on safety procedure to the employees and provide appropriate working equipment.

Bow tie analysis also analyse the consequences of every risk when it happens. In the case of injury, since there is only one person normally working in the store, so if that person get badly injured and cannot continue his work, it will certainly disturb the company business operations and in worst case, that person can sue the company because the company fail to provide appropriate working equipment or first aid kit to treat the wound.

In addition to that, by knowing the risks, the company can then implement the corporate security areas to protect its valuable assets as the corporate assets nowadays are bombarded by threats from inside and outside the organization. The goal of the corporate security is to provide protection and security measures to manage the risks. The corporate security areas: Production and Operation Safety, Occupational health and safety, Environmental safety, Rescue Operations, Contingency Planning, Information Security, Personnel Security, Physical Security,

Security of International Operations, and Crime Prevention has its own function to protect the valuable corporate assets.

For example by implementing the areas physical security, the company can review what kind of protection it has regarding physical security and what kind of development program it needs to have if the case study company wants to protect its business.

5 Summary

This thesis has managed to identify, prioritize and thoroughly analyze various threats that exist within the case study company. Furthermore, it provides the path and various suggestions towards the existing threats and risks that are potentially disturbing the business continuity of the company.

With the analytical approach through observation and experiencing the daily operation, added with in-depth interview (appendix 1) with the store manager and the CEO of the company, the author has managed to classify the practical and, in some cases, hidden threats to the company.

The risks, divided in external and internal, have emerged from those methods with various level of possible loss to the company and in needs of solutions. It is through an appropriate method of ALE and bow-tie analysis that all the risks are analyzed in a comprehensive manner in regards of its causes, preventive measures, and its importance to the case study company.

After proper analysis of ALE (table 3 & 4) and the in-depth analysis of bow tie (figure 12 - 19), this thesis provides a groundwork for the case study company to acknowledge the various areas that are still vulnerable to threats and offers the possible paths and measures that can be taken in order to increase the business resilience of the case study company. The ALE provides a better priority of the risks so that the case study company can have a higher awareness to the most critical problems, and bow-tie serves as a well visualized method of thorough explanation regarding each of the risks.

The protection of corporate assets through various aspects of corporate security is also being analysed in addition to all of the methods. By knowing the major corporate security aspects of the case study company (appendix 2), it can also provide an additional solid foundation for the company to increase its resilience towards disturbing events and risks.

Furthermore, the increase of business resilience and high awareness of threats that can possibly affect the business continuity of the case study company will optimistically increase the chance of higher profit margin of the case study company in the long term.

References

Book Sources:

Blyth, M. 2009. Business Continuity Management: Building an effective incident management plan. New Jersey: John Wiley & Sons Ltd.

Hotchkiss, S. 2010. Business Continuity Management: A Practical Guide. Swindon: British Informatics Society Ltd.

Hopkin, P. 2012. Fundamentals of risk management : understanding, evaluating and implementing effective risk management. 2nd Edition. London: Kogan Page Limited.

Elliott, D., Swarts, E. & Herbane. B. 2010. Business Continuity Management: A Crisis Management Approach. 2nd Edition. New York: Routledge.

Sandhu, R. 2002. Disaster Recovery Planning. Ohio: Primer Press.

Wallace, M. & Webber, L. 2011. The Disaster Recovery Handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets. 2nd Edition. New York: American Management Association.

Gill, M. 2006. The handbook of Security. New York: Palgrave Macmillan.

Kovacich, G. & Halibozek, E. 2003. The Manager's handbook for corporate security: Establishing and managing a successful assets protection program. Massachusetts: Elsevier.

Sterling, S., Duddridge, B., Elliott, A. et al. 2012. Business Continuity for dummies. West Sussex: John Wiley & Sons Ltd.

Norman, L. 2010. Risk Analysis and Security Countermeasure Selection. Florida: CRC Press.

Electronic Sources:

Thoma, K. 2014. Resilience by Design: a strategy for technology issues of the future. < http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Stellungnahmen/acatech_STUDIE_Resilientech_WEB.pdf>. (Accessed 24 March 2015)

Yritysturvallisuus. <http://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/>. (Accessed 20 January 2015)

Cooke, A. 2013. Do you have the 3 factors for organizational resilience?. < http://growthandprofit.me/2013/02/04/do-you-have-the-3-factors-for-organizational-resilience/>. (Accessed 22 December 2014)

Business resilience: The best defence is a good offense. 2009. <http://www.ibm.com/smarterplanet/global/files/us__en_us__security_resiliency__buw03008usen.pdf>. (Accessed 04 January 2015)

Birkinshaw, J. 2012. What Makes a Company Resilient?. <http://www.businessweek.com/articles/2012-10-16/what-makes-a-company-resilient>. (Accessed 06 January 2015)

Figures

Tables

Appendices

Appendix 1: List of Interview Questions

1. Can you please explain little bit about the company business values?
2. What do you consider as the company assets? Can you rank the importance of them?
3. In your opinion, how the three factors (flexibility, adaptability, and learning) of business resilience affect the company business operations?
4. What do you think about the company current situations regarding threats?
5. In your opinion, what are the company internal and external risks?
6. Could you please estimate for every risk mentions in the external and internal risks, how big is the impact for the company in terms of money?
7. What do you think about the frequency of occurrences for every risk?
8. What do you think about the risk related to the employee that shows low result in the ALE analysis?
9. In your opinion, what the company has done to protect their assets in regards of the corporate security areas?

Appendix 2: Corporate security of the case company

Areas	Case company	Area to develop
Production and Operation Safety	Since the company did not produce anything, therefore this area will only cover the safety of operations in the store and with the suppliers. According to the store manager, the company has always checked the quality of products delivered by the suppliers, both dry goods, e.g. flour or beans, and fresh items, e.g. vegetables and fruit, to ensure the product is safe to be consumed by the customer. The company also has a regular checking done by the manager on the temperature of freezer and refrigerators to ensure the products are stored within the right temperatures.	1. Employee training in basic food safety, including training on hygiene practice, proper temperature control and food handling. At the moment, only the manager knows how to handle the goods. Thus when the manager is not around due to business abroad, no employee is able to perform the proper checking of the products. 2. To reduce loss of profit because of expired items, the company needs to have training regarding product expiration. The training will cover the right way to display the products, how to handle products that are nearly expired, and how to handle products that have expired both in the store and in the warehouse. It is important because according to the manager, the company has lost certain amount of profit because the employee who is in charge in the warehouse and store did not pay attention to the products. Many cases, the employee places the products with longer expired date on top of product with short date. 3. Hire extra employee to come at least

		once a week to check the product expiration and clean the store. At the moment, there is only 1 employee handling everything in the store. The person is responsible for ordering goods from warehouse, cleaning the store, taking order from business customer, working as a cashier, putting a price tag in products, etc. During a busy day, the responsible person is unable to handle all tasks, thus in most cases, he/she will give up cleaning and it leaves the shop dirty and unarranged.
Occupational health and safety	Based on the observation, the company needs to improve the occupational health and safety. Even though the company has insurance for all the employees, and providing appropriate working hours, it is seen as not enough. The company needs to develop this area since it covers the health and safety of the employees within the shop. Therefore in the next table, the reader will find suggestions from the author to the company.	1. Provide appropriate working equipment. For example, gloves for the employees when handling frozen/fresh items. Additionally, currently the store has only one broken ladder and it is still used daily to take some products that are in high area. It is recommended that the necessary working equipments area updated as soon as possible before injuries happen due to using the broken ladder. 2. Provide the first aid kit tools in the store. Oftentimes when employee gets injured (cuts or sprains their muscle) or experiencing a headache, they are unable to treat themselves because there is a lack of basic medical items.
Environmental safety	In regards of the environmental safety, the author concludes that the store has tried to have a safe working environment	However, to support more friendly environment, the company is advised to: 1. Sort the waste. At the moment, the company has only 1 big recycle bin. So all the waste is placed in one big plastic

	and ecological friendly by keeping all cleaning utilities and chemicals in separate places and providing clear labels for chemicals. In additional, every two days the employees remove the entire empty boxes from the store and bring them to the recycle place to keep the store clean.	bag regardless of its material (metal, glass plastic, bio, paper, etc). 2. Develop guidelines and procedure on how to recycle waste. 3. Create necessary document on how to handle dangerous chemicals.
Rescue Operations	At the moment the company has only emergency exit sign placed in the store that can be used as direction to leave the store during a fire or other disruptive situations.	1. Create a security plan that covers the rescue plan during disruptive events. 2. Installation of safety equipment. For example fire alarm, smoke detectors or fire sprinklers. 3. Have a periodic inspection of the rescue equipment.
Contingency Planning	According to the manager, so far the company does not have any proper contingency plan and no written documents regarding the business continuity during disruptive events. The manager said that if something happens to the store, the employee will inform the owner of the case company and then he will decide what to do next. So for example, if	It is important for the case company to have business contingency program to ensure business resilience. The contingency program will include: - Emergency response - Crisis management - Business continuity By having a contingency program, the company will have a preparation in a case of disruption. It is also able to protect the company by implementing certain strategy to reduce their loss and by having the plan, it can decrease the probability of confusion as employees have been informed and re-

	there is a fire and causing one of the shops to close down, then the emergency plan is to move the business operations to the other store.	hearsed as to what actions to take during an emergency situations.
Information Security	The company has implemented basic information security in its business activities. It can be seen by: password requirement to open company's private computer, use of antivirus in the computer, barrier (doors and locks) to get into the manager office, etc. However, the data is still scattered and not classified based on its confidentiality. Therefore, the company needs to develop strategy to prevent disclosure of information by the employees due to lack of information regarding the information confidentiality.	The case company is recommended to: - Classify the information based on the level of confidentiality. The classification system can help the employee to distinguish which data is part of the general information, which data is considered as internal and confidential. - Once the data has been classified, the company needs to set access control to prevent unauthorised person to access the data. For example: general information can be accessed by everyone, internal data can only be accessed by employee, confidential data can only be accessed by the manager, etc - After the data has been classified and create necessary access control to it, the case company is advised to create security procedure or policy to protect each data or information that are not yet included in each classification category.
Personnel Security	The personnel security is important because it can protect one of the company's valuable assets, the employee. Currently, the company is running a necessary personnel security by having	Recommended actions regarding personnel security are: 1. Development of policy on threats or acts of violence. The policy can be used as a foundation for the company to do disciplinary action including termination of employment to ensure safe working environment 2. Pre-employment background check:

	basic security training for the new employee. The manager makes himself available to the employee in case there is an issue in the workplace.	This process is useful to reduce the chance of hiring potentially violent and criminals.
Physical Security	Based on observation, the company has been using the appropriate physical protection to protect their valuable assets. Example physical barriers that they have are doors, walls, surveillance camera, access code, and alarms.	However, there are certain areas of physical security they can still develop: 1. There are several blind spots in the store where the CCTV could not observe and record the areas. Therefore, it is advised that they install 1 more surveillance camera to increase the protection of store. 2. The shop does not have adequate lighting. There are some broken lights in the shop that have not been changed. Sufficient lighting reduces the possibility of accident and injury. With enough lighting, the shop areas, walls, entrance can be clearly observed. 3. At the moment, all the employees have same security code to unlock the alarm systems in the store and warehouse. The company is advised to provide different code for different employees and request the employee to keep it safe and not share it with other employees. The function of different code is to keep track which employee arrives first to the store and which employee that leaves the last. It is as well to know which employees that come and go to the warehouse.
Security of International Opera-	There are no employees that are travelling abroad	At the moment the company does not seem to need the procedure that guides business

tions	due to business work. Only the owner of the company usually travel abroad to have a business meeting. Therefore they have not implemented the safety of international operations.	travelling. However, it is recommended for the company to pay attention to it since the company is growing all the time and there are possibilities that the business will expand. Therefore, the author proposes the ideas to: - Create policy and procedures for travelling abroad - Train the employee regarding travel dangers and how to act during an emergency situations abroad - Since it is the owner of the company who usually travel abroad, it is wise for the company to create separate executive protection for the owner of the shop. Because the lost of company owner can have a serious and adverse impact on the business operations.
Crime Prevention	The case study company has done retail loss prevention by installing surveillance camera in the store, training the employees regarding shoplifting, and especially to pay more attention to the customers that look suspicious, or taking too much time in the shop. The company also has a security button that connects to security company. The employee can press if they feel threatened or if there are any criminal activities going on in the store.	As mentioned earlier in the physical security, in order to prevent criminal activities, the company needs to install another camera to cover blind spot area. Create clear policy and procedure regarding criminal activities. Since the company sells expensive cosmetic product, they can start thinking about the installation of alarm system especially for the expensive products.

Appendix 3: Glossary

Business Continuity: Effort to minimize business disruption caused by different threats. (Hotchkiss 2010)

Disruptions: The period during which some part of the business operation does not work due to unexpected situations or event. (Hotchkiss 2010)

Likelihood: Chance of something happening. Sometimes it is referred as frequency or probability. (Elliott et al. 2001)

Mitigation: Action taken to reduce the impact of a risk. The impact can be reduced either by providing alternative option or by fixing the problem. (Hotchkiss 2010)

Resilience: Ability to prevent or mitigate threats by being well prepared and taking appropriate measures to response the threats. Resilience can be defined as the ability of business to endure unpleasant events and guarantee business survival. (Thoma 2014)

Risk: An event that could have an impact on the fulfillment of corporate objectives, strategies, projects, core processes, or missions when it occurs. (Hotchkiss 2010)

Risk identification: A process of finding and recognizing risks by identifying the risk sources, events, their causes, and potential impacts. (Hopkin 2012)

Risk analysis: A process to understand the character of risk and to determine the level of risk. (Hopkin 2012)

Risk management: A system on the organization that enables the company to identify potential risks, evaluate them, identify solution to reduce or prevent the risks to occur, and prioritize the risks. (Hopkin 2012)

Risk matrix: Presentation of risk information on a grid or graph, also sometime referred as a risk map. A risk matrix classifies risks based on the impact and probability of occurrence. (Hopkin 2012)

Threats: Things that can go wrong and disturb the organization, e.g. fraud or fire. Threat can affect to people, process, physical assets, buildings, etc. If the organizations not mitigate the threat, it can cause business disruption. (Hotchkiss 2010)