Välikangas Jane

The role of the CEO in a company's information security

— in small-sized technology companies

Master's Thesis in information systems
Supervisor: Prof. Anssi Öörni
Faculty of Social Sciences, Business, and Economics
Åbo Akademi University

Turku 2022

Abstract for Master's thesis

Subject: Information Systems
Writer: Jane Välikangas
Title: The role of the CEO in a company's information security
Supervisor: Professor Anssi Öörni
Abstract: The role of the CEO in a company's information security changes as more cyberattacks and data breaches occur. In today's business world companies of all sizes have to consider information security. In Finnish companies information security is usually thought of after an attack not before as it should. The purpose of this study is to gain knowledge about how the CEOs themselves think about information security in the company and their role in it. The focus is on information security management and corporate risk management, especially the difference in management and responsibility. The sampling method is purposive sampling and the characteristics of six respondents were the CEO of the company, a Finnish-based company, a small-sized company, and the company is in the IT business field. The method used is qualitative research with semi-structured interviews. The research questions were created from the literature review. The used theory is grounded theory, which provides the research freedom to change the theory with the results. The analysis of the research responses is coding where the responses are compared with each other and to the literature review. As the results conducted, the CEOs think that when it comes to risk management they are in the end the one who is responsible, however, in information security there is usually someone else who is responsible for those actions. As the results suggest, awareness of information security among the CEOs needs to be more considered.
Keywords: Information security, corporate risk management, cyberattack, data breach, vulnerability, threat, The role of the CEO, risk management model, responsibility

Date: 19.4.2022	**Number of pages:** 92

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

1 INTRODUCTION

Scamming, ransomware, and data breaches are the highest-profile cyber incidents. They are a regular threat to companies and are occurring all around the world. When a company is a target for a data breach, usually employees' and customers' confidential data are lost to an attacker. The attackers may attempt identity theft with the stolen data of the customers or employees. For the victims of the data breach, this creates harm and worries when the attacker uses stole data. Furthermore, data breaches can harm companies and their reputation (Coburn, 2018).

In today's business world, information security is an important part of technology, and it is continuously evolved by those who are using it. The level of misuse of data has increased as the level of companies collecting data from technology users has increased at the same rate. This has led to cyberattacks, e.g. phishing attempts outside of the company have become an everyday issue for organizations (Coburn, 2018).

The term risk management refers to a company aiming to identify its vulnerabilities and assess the threats towards such vulnerabilities. A risk management strategy implies that a decision about the security of the company is based on mandatory requirements by a government and the expenses of information security are determined. A company's security and the cost of it must be balanced. Risk management is a necessity for the company. Without risk management, the continuity of the company is threatened (Colwill, 2010).

A CEO determines who is accountable for different actions in the company. The role of a CEO, however, varies depending on the size of the company. In a small company, the responsibilities are more extensive and a CEO has a variety of tasks to implement. Whereas, in larger companies with more employees, a CEO can delegate tasks to others which will remove responsibility from the CEO to other employees.
Managers in Finnish SMEs have multiple roles within a company. Some information security tasks are delegated to lower-level managers, as a CEO is not able to manage everything alone. Delegating tasks do affect information security in the company as numerous employees or departments might be accessing important information which might affect the management of information security. The larger the company size, the

greater the amount of information to be secured. The size of the company matters in information security as medium-sized enterprises are the ideal target for scams. Small-size companies are not worthy of the cyberattacks and larger companies might have prepared well for the cyberattacks (Iannarelli & O'Shaughnessy).

This master's thesis analyses the field of information security from a CEO's point of view. The focus of this master's thesis is on Finnish SMEs. The research was executed by interviewing Finnish SME CEOs. The method used is qualitative research and the interviews were implemented with semi-structured open-ended questions. The respondents were asked about their opinions and ideas concerning information security and risk management in their companies. Grounded theory and a theoretical framework are theories used to analyse the responses of the CEOs. The interviews aim to gain further practical knowledge of the responsibilities in the case of a data breach or cyberattack in a company. Furthermore, the interviews seek to receive further knowledge on what CEOs think about their responsibilities towards the company today and to receive knowledge about their hopes for the future of information security.

As a theoretical framework for the interviews, the thesis comprises a literature review, consisting of three parts, i.e. information security, corporate risk management, and the role of a CEO. These chapters aim to understand the responsibilities of the CEO regarding the company's information security.

1.1 Objectives of the master's thesis

The idea for this master's thesis came from the researcher's interest in the subject. Previous researches on the responsibility of the CEOs in Finnish companies are not so common, especially in the field of information security. The CEOs' awarenesses of information security and risk management are the key concepts that are analysed separately and then compared with each other. The objectives of this research are to collect the different thoughts and ideas of the CEOs regarding information security and risk management especially when it is about the responsibility towards those. The selection of these two topics is the key to this master's thesis. The reason information security and risk management are chosen topics from the CEO's point of view is to see the difference in the management and responsibility between these two topics.

Information security is more related to IT and it is intangible information and corporate risk management is more communal and is tangible information. Both of the concepts are wide and a lot of information exists already. The concept is first presented and the concept of the role of the CEO in the interview is combined with the research questions.

The interest in the subject comes from a real-life example such as the case of Vastaamo (Yle, 2020), which is a private psychotherapy centre in which customers' information was hacked and leaked onto the web and some victims received ransomware. From this example came the central question of this master's research.

The key research questions are:

- *Who is responsible if a cyberattack or data breach occurs in a company?*
- *Who is responsible if an action is executed by an employee after an incomplete or non-existing policy and this action will affect the company negative?*

With these objectives, the study researches the ideas and thoughts of CEOs today. At the same time, the CEOs responded to their future hopes with the company's responsibilities for information security. They all concur that cyberattacks are increasing, and they are issues to take into consideration now and in the future.

1.2 Structure of the master's thesis

This study consists of six chapters. Chapter 1 contains an introduction and the structure of the thesis. Chapter 2 presents the theoretical framework for the thesis. It consists of literature reviews on information security, corporate risk management, and the role of the CEO in a company. Each of these subjects is reviewed from the general perspective and with a focus on the perspective of the CEO. Chapter 3 presents the research method and design. In this chapter, the method used for the research and the analysis of the responses is further presented. Furthermore, the sampling method explains how the respondents were selected and the characteristics of the respondents' are presented. Chapter 4 discusses the results of the CEOs' responses. The responses were collected and encoded in groups to identify the similarities and differences. Grounded theory is

used for the entire interview and to analyse the responses. Chapter 5 assesses the results and summarises them together with the theoretical framework to establish a theory of the CEOs' ideas about information security in Finnish SMEs and the responsibilities of a CEO in a company. This chapter also proposes future suggestions by the CEOs on how information security should be handled in companies and what should be executed differently in the future. The final chapter, Chapter 6 concludes the whole master's thesis and summarises it.

2 THEORETICAL BACKGROUND

Chapter 2 introduces the literature review providing a theoretical background to this research. The theoretical background covers the definitions of the main concepts of this study and presents the observations and key findings made from previous studies. The theoretical background consists of three parts which are information security, corporate risk management, and the role of the CEO.

The topic of information security and corporate risk management are wide concepts that are presented first from a general perspective in the theoretical background. This provides the reader the information to understand the role of the CEO with these concepts. The last part of the theoretical background is the role of the CEO. For the reader, this provides information about the selected respondents and what is the role of the CEO. All of these three concepts are combined in the research questions when interviewing the CEOs.

2.1 Information security in the company

Information security is the protection of systems and assets with different policies, controls, and software along with other related solutions. Information governance lays out a framework that bridges these gaps together (eDiscovery).
Information governance has many aspects such as systemic solutions to counteract threats, alleviate inefficiencies, and prepare for the future. Governance of information is a broader entirety than an IT problem, which usually is more of a technical issue. IT-term as referring to information technology can be understood in several manners and there is not only one understood definition, it has many. Thus, when observing the different actions of IT, multiple actions can be noticed. IT, as part of the governance of information, has multiple issues to consider which vary from only IT-related issues to wider issues (Iannarelli & O'Shaughnessy, 2014).

Cyber threats imply more than that one attacker using a computer and monitoring others from a faraway distance. This entails that the larger the threats businesses have to be concerned such as a threat to a company's confidential information, either clients or business itself, the greater the risk of a third party information exposure increases.

Moreover, where a cyber threat occurs, there is a great risk of causing major damage to the reputation of the business, whereas a company that would be targeted for information leaks, is probably encountering financial damage. For a business owner, both the reputation of the company and financial issues are crucial as they all affect profit-making. Meanwhile, scammers are learning to be smarter and wiser, and the users are required to be careful with the information they are providing to the companies. On some occasions, despite the company maintaining the information security plan, the breach might be by the customers' action (Iannarelli & O'Shaughnessy, 2014).

2.1.1 How company size affects information security

As the size of SMEs is small,- or medium-sized, employees and managers have multiple roles, this entails that in SMEs CEOs delegate decisions to other employees and managers. For a company to be successful the company must use an information governance program and a corresponding communication program. When using those programs, those delegated decisions must be taken into consideration (Iannarelli & O'Shaughnessy, 2014).

The larger the company size, the larger is the number of threats that could occur, and also the number of important information that requires to be secured inside the company. This applies also to numerous employee data. Thus, with the larger number of employees working in the company, the risk of a human error increases. In addition to such internal security threats, threats from outside of the company are increasing as cyberattacks may occur every day and the company has to be prepared for them. Often threats occur more in medium-size companies due to their ideal size for scamming. Into small-size companies, on the contrary, are not worth the effort of attacking, and larger companies' IT systems might be difficult to penetrate (Iannarelli & O'Shaughnessy, 2014).

Considering that the primary focus should be on business. A company must find a balance between protecting the data and being a profitable company. Furthermore, for the business to be successful, its reputation should not be harmed. Thus, focusing on IT security ensures the continuity of the business (Iannarelli & O'Shaughnessy, 2014).

The majority of the SMEs have faulty ideas of their security and the information related to security. In a survey (McAfee's 20081) of 1100 respondents from the U.S and Europe, more than half thought only large companies can become subject to cyberattacks. This assumption led attackers to focus more on not-so-well-protected mid-sized organizations. As a result, attackers have been able to access companies' sensitive data as the companies do not understand the importance of information security (Král, 2011).

2.1.2 Certifications and government regulations

For larger companies, security certifications have a great impact on information security. Certifications aim to guarantee a certain quality of security and ensure a certain consistency with other management systems of an organization. Certification standards are in general not something SMEs apply for. Certifications create demand from administration, and the application process for certification is often unnecessary and burdensome for small businesses. However, for a medium-sized organization, certain administration associated with information security is a necessity. In small companies that are often family-owned or where employees are otherwise familiar with each other, a certain degree of anonymity might, in turn, lead to employees not respecting security procedures. In general, in the majority of the cases concerning the misuse of security procedures, the procedures had not been clearly defined or checked by the company. Consequently, certifications can be helpful for companies with unclear security procedures. Their advantage, however, depends on the organization and the establishment of an internal methodology for information security (Král, 2011).

The majority of industries are regulated by the government in terms of how to handle and use data. In principle, companies will ensure that they have the information they must require and nothing else, document types and formats are correct and companies receive a track of the retention rules. Regulations and compliances become a threat only when regulations are not followed, and compliances are not maintained.
Corporate governance is in general understood as a term referring to finances and the future of an entity, not as something affecting most of the employees in the field. The management of data information is considered equally unimportant. Regulations regarding data companies have about their customers and employees are nevertheless

useful. Without such regulations, companies would have more breaches occurring (Iannarelli & O'Shaughnessy, 2014).

2.1.3 Cyber security – An outside threat

Companies suffer from cyberattacks or system failures in the IT sector in several ways. For companies, losses after a cyberattack might be disruption to business operations or added extra costs. By preventing cyberattacks, companies are preventing the risk of different types and levels of losses. Key loss processes are data exfiltration, contagious malware attacks, the denial of service attacks, financial transactions, theft, and failure of counterparties or suppliers. These key losses cause roughly 90% of all business losses in cyber security (Coburn, 2018).

2.1.3.1 Data breaches

Data breaches are the highest-profile cyber incidents. Data breach entails a company losing its confidential data from customers, employees, clients, or counterparties to the attackers. If the data a company is holding becomes available for the attackers, it might reveal some sensitive information about the business. That information might bring a competitive advantage to the company's rivals. Furthermore, if the information is published by the attacker, it might ruin the company's reputation and a company may lose customers or projects as a result of the data breach. Moreover, in terms of personal data, especially identification credentials, payment card information, or health care information, the consequences might be serious, whether the personal data were customers' or employees'. Misuse of stolen data entails a variety of actions, such as identity theft, fraudulent transactions, stealing money, blackmailing, or being held for ransom by the attacker. Companies are subject to strict regulations by the government as to how to act in case of a data breach. A company has to make a public notification about identifying the records that have been lost and notify the individuals concerned. The company is also required to assist the victims in managing the consequences of the breached privacy, and pay financial compensation (Coburn, 2018).

Unfortunately, data breaches are currently more common than before. Attackers are becoming to be cleverer than before, resulting in it has become more difficult for users to recognize which attempts are scamming and which are not. In Finland, the most well-known case of hacked customer information and ransomware is the Vastaamo case

(Yle, 2020). The case concerns a private psychotherapy centre in which customers' information was hacked and leaked onto the web and some victims received ransomware.

In 2005, around 8000 U.S enterprises had been affected by cyberattacks, involving numerous structural characteristics and security measures that cost companies much harm and costs. A survey by Human et al. (2021), reveals that enterprises are not equally affected by cyberattacks, thus the enterprise sector validates which sectors are frequently targeted. Companies outsourcing all or part of their computer security had higher prevalence to be targeted for an attack. According to the UK Department for Digital, Culture, Media & Sports article "Cyber Security Breaches Survey 2019" a third (32%) of the participating businesses experienced a cyber security breach or attack in the past 12 months. Also, the survey reveals that large businesses are at a higher risk of being attacked. Similarly, some sectors suffer more from online crime incidents than others. Research, conducted by Huaman et al. (2021) examined medium-sized companies in Germany, and they interviewed the employees of the companies about their knowledge of different aspects of security. Researchers have found that employees have a basic knowledge of the company and its risks and threats. Thus, companies have the awareness concerning information security, however, the knowledge has not reached all the employees.

2.1.4 Cyber security – An inside threat

To exploit vulnerabilities and steal information from inside a company is more cost-effective than launching an attack from the outside, as the latter requires penetration through multiple layers of protection. The attackers from inside a company have time, capabilities, and opportunities to create an attack. In general, protecting information and data becomes complicated when a third party is involved through outsourcing. Furthermore, outsourcing information security might lead to the extension and potential dilution of the controls and protections. When third parties are provided with the same privilege and access rights as an insider, new opportunities for threat actors to identify the information and vulnerabilities of the company are created (Colwill, 2010).

In comparison to outside attacks on a company, far less factual data exist on inside attacks. According to the US National Infrastructure Advisory Council, awareness and

mitigation of insider threats variate highly among companies and sectors, and in most cases, they are addressed poorly. Also in the UK, numerous organizations are not considering information security enough to protect themselves and their customers' information. Among others, the following acts are poorly executed within companies:

- 52% of the companies do not carry out any formal security risk assessment
- 67% of the companies do nothing to prevent confidential data left on USB sticks, etc.
- 78% of the companies had computers with unencrypted hard disks stolen
- 84% of the companies do not scan outgoing emails for confidential data.

Consequently, the majority of the security incidents which occur are accidental. Accidents can have a greater impact than malicious insider attacks. In total, 52% of insider incidents were accidents, including 6244 incidents of unintentional data loss (Colwill, 2010).

According to Colwill (2010), the underlying reason for inside incidents is that organizations now understand the threat is real, though they are not aware how to handle inside threats. On the contrary, the threats coming from outside, such as hacking or insertion of malware from an external source are more familiar to the public. The threats from outside have known signs and, they are widely reported and discussed.

2.1.4.1 Outsourcing

Outsourcing is common for a company to survive in today's increasingly competitive business environment. The majority of companies must confront mandatory transformation to outsourcing. As the results of this, third-party personnel having access to an organization's critical system's information is rapidly growing. Thus, a company's transaction with outsourcing can change the status of outsiders into insiders and blur the line between the company's employees and third-party personnel. In some cases, the security components are outsourced instead of the employees. Outsourcing can furthermore be offshore or onshore. Using both methods increases the number of third parties and contractors (Collwill, 2010).

Long-term access is provided for outsourced employees to a company's critical systems and information. Offshoring information may create an aggregation of data from

numerous regions and centres. Offshoring may also create an opportunity for a malicious insider who has access to the sets of information. Contributing to offshoring parties who have no responsibility or understanding about the implications used, will not be undetected by them that it may create an opportunity for a criminal, foreign intelligence services, and terrorists (Collwill, 2010).

A human threat can be divided into the factors of motivation, opportunity, and capability. The employees' responsibility is to protect the organization's data. Education, training, and creating awareness can be ordered by companies to achieve information security among employees. Security integrated into an everyday work environment is important. Further, clear policies and employee training are mandatory to raise awareness among employees. Although several insider issues are based on ignorance rather than malicious motivation, ignorance does not delete the consequences. Accidental failures can have a great impact on the continuity of a company (Colwill, 2010).

2.2 Corporate risk management

Risk management is identified as an act of identifying risks that are specific to the organization and responding to the risks accordingly. The stages of risk management are identification, assessment, planning, and managing of risks. To have effective risk management, all levels of the organization are included in the process. Such levels are corporate, strategic business, and the project. Risk management aims at identifying risk, undertaking an objective analysis of risk specific to the organization, and responding to the risk accordingly (Merna & Al-Tani, 2008).

2.2.1 Corporate risk program

A corporate risk program is important for a company. A company shall assign at least one employee who maintains the corporate risk programs and engages in risk management daily inside the company. Every employee should know at least the guidelines of risk management as it affects the continuity of the company. Employees should know at least how to recognize risks and how to handle them on daily bases in the work environment (Campbell, 2014).

According to the CISA Review Manual 2006, "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take into consideration when reducing risk to an acceptable level, based on the value of the information resource to the organization". The risk management process is thus an ongoing iterative process and its timeline is indefinite. In a business environment, changes and new threats and vulnerabilities emerge daily. With controls or countermeasures exist a demand for a balance between productivity, cost, the effectiveness of the countermeasures, and the value of the informational assets which are being protected (Sattarova & Tao-Hoon, 2007).

The term *risk* refers to the likelihood of something negative occurring, that will cause harm to informational assets or their loss. Different types of risks, vulnerabilities, and threats exist in the corporate environment. Vulnerability can be described as weakness that could be taken advantage of to endanger or cause harm to the informational asset. A threat in turn refers to something man-made or to an act of nature that can create potential harm. The impact results from a threat that causes harm to vulnerability. In information security, such an impact requires a loss of availability, integrity, and confidentiality. The risk can result in the possible losses of income, with life, or property. Commonly, it is not possible to identify or eliminate the risk and the remaining risks are called residual risks (Sattarova & Tao-Hoon).

The ISO/IEC 27002:2005 *Code of practice for information security management* recommends the following issues to be examined during a risk assessment:

- security policy
- organization of information security
- asset management
- human resources security
- physical and environmental security
- communications and operations management
- access control
- information systems acquisition, development, and maintenance
- information security incident management
- business continuity management

• regulatory compliance
(Sattarova & Tao-Hoon, 2007)

Companies have not taken as much notice of security risk management in the past. Rather, issues with threats were solved by a technical solution. In the early 21st-century researchers began to realize that this was not the correct solution. In security risk management, technology and economic issues demand attention simultaneously. Business managers developed an advanced understanding about security investments with the economic aspect. Consequently, the technical analysis of the implications of security failures was replaced by an analysis' of economic losses. Knowing information security risk management raises several questions, such as *which security level is adequate? How much money should be invested in security?* (Bojanc & Jerman- Blažič, 2013)

A false sense of security can be noticed as an ineffective focus on threats. The ineffective focus results in risk management converging to inside danger. Risk management should be aware of the vulnerability acts and sources that will not exploit insiders. The focus is on ensuring that risks associated with insider attacks are qualified and quantified. Risk management also includes identifying cost-effective mitigations. Furthermore, to succeed in risk management, an organization has to ensure the employees' awareness with questionnaires and scenarios for the threats to occur, and identify employees who can cause a high impact of human error. Therefore, human behaviour must be explicitly taken into account in the context of changing technical, social, business, and cultural factors in a company (Colwill, 2010).

2.2.2 URO & ERM

Unified Risk Oversight (URO), or corporate risk is a method of identifying the company risks by the business units. Managers or teams of executives identify threats based on the ideal results and findings inside the team. Achievements in the business goals have to be succeeded, for a company to be successful, and not to lose the already made achievements. A company will revise the whole business and not individual units. Comparing risk evaluation with other business units is common for the company to be able to find the similarities and view which risks are ideal to be prioritized (Campbell, 2014).

Corporate risk is often referred to as enterprise risk management (ERM). The difference between URO and ERM relies on how ERM impacts the board level, whereas URO focuses more on facts or entities that cover the entirety when all the units are identifying their risk themselves. In the URO approach, the lower-level managers are also involved with corporate risk management. URO entails a full consideration of the impact of actions on all business units. Risk is managed with centralized thinking and the decision-making process, including, acceptance, avoidance, or transferring. Decisions affect all business units in a company. Furthermore, security is considered and it is reflected in the decision, which seeks to provide an ideal outcome for all the business units (Campbell, 2014).

The process for enterprise risk management includes eliminating or minimizing uncertain events that could prevent business goals from achieving. Before eliminating or minimizing such events, the risks have to be identified and controlled. This process requires the identification and evaluation of the company's information assets. Information assets refer to an assessment of the effects of security incidents, an assessment of the likelihood of a successful attack on the information system, and a business assessment of the costs and benefits of an investment in a security solution. The risk management process includes various stages such as identifying vulnerabilities in an enterprise information system, evaluating the potential security protection, deciding on acceptable risk, and choosing appropriate cost-effective protection. This process aims to create a proposal for a price not exceeding the expected loss that can be caused as a result of an attack. In general, the process consists of two main stages, which are risk assessment, and risk treatment (Bojanc & Jerman- Blažič, 2013).

2.2.3 C-level managers in risk management

Ultimately, it is c-level managers, such as CEOs that ensure the correct performance of the security policies. According to Speed (2011), c-level managers are at the top of the company and, they decide on policy creation, funding, and implementation. C-level managers are invaluable for the company's information security as they provide the leadership which is demanded to create and implement policies. A C-level manager oversees all the departments in a company and, therefore, knows how different regulations affect the whole company and every unit of the company. If some regulations do not function in one department, the C-level manager can make changes

without reforming the whole regulation in the company which is time-, and energy-consuming. A C-level manager is a crucial player in the company, considering organization-wide policies and being involved in security issues.

According to Speed (2011), C-level managers are responsible for corporate accountability, including risk management. C-level managers thus look after decisions that have been made and verify that the decisions are approved by the shareholders if the company has any. The CEO has to confirm that the governmental rules and regulations have been adhered to that ethics and morality are considered and that the employees are aware of how they can affect their tasks. According to Speed, if an employee's actions affect the company negatively and executed action was executed as a result of an incomplete or non-existent policy, then a C-level manager is accountable for the damage or loss.

2.2.4 Assets

For the majority, the word *asset* is understood as a physical realm, such as facilities, real estate, desks, computers, and other equipment. Physical assets help the daily operations to preserve and run a company. Physical, tangible assets can be measured by their value and, they affect from the lowest-, to the top-level of the organization. Intangible assets, such as collected data, ideas, customer contact information, or even employee records, in turn, are great assets for companies. An asset is any information beneficial to a company, hence an information asset. An information asset is presented as information that is not meant to be notified outside a company, as one would cause damage to the organization with it (Speed, 2011).

The culture of security awareness is something that every employee in a company, from top-level to lower-level employees, should be aware of. Employees have to carefully protect the assets and interests of the company. Thus, a company must establish culture and knowledge awareness to maintain the security of information assets. Creating such a organization culture is often simpler than assumed, as the core of building a workforce culture is knowledge about security issues. In general, every employee should know the organizational assets and the possible risks towards those assets. When employees have the knowledge and information about the assets of the company, they also feel more immersed in the culture of security awareness. In general, security awareness has more

positive effects than negative. It enables small accomplishments to be achieved, rather than resulting in greater issues than the negative effect of employees' unawareness. Rules have to be the same for everyone. Employees who know their position in a company, also know what they are supposed to or not to do, according to the security awareness (Speed, 2011).

The critical aspects of an organization are security, safety, compliance with business processes, and involved assets. In a supply chain process, partners want to ensure that the purchase order data and payment data are correct. Furthermore, partners want to be ensure the ordered goods are treated according to various requirements. To achieve such assurance, partners require treating assets accordingly, ensuring that the circumstances are correct, and doing checks during the process (Monakova et al. 2012).

Threats have different impacts on information assets. A threat focuses on the destruction of information assets, the change of information assets, the theft of information assets, the disclosure of confidential information, and interruption of service (Bojanc & Jerman- Blažič, 2013). Virtually it is impossible to know which assets will be interesting for an attacker due to the changing nature of risks. Thus, an asset that is ignored today might be interesting for the attacker in the future. Changing the nature of risks creates an effect of the risk shift on unexpected organizational areas. Furthermore, the prediction of risk can be problematic, as the risk is an uncertain outcome, and can have both positive and negative impacts. Moreover, risk tends to provide more frequency and magnitude of loss. The danger exists in putting negative security risks, i.e. losses, in the context of positive risk, i.e. gain, and accepting possible detriment or damages. As information security management is a multidisciplinary field, a solution to this problem must be sought in various fields that often subdivide into partial problems of different origins. Risk assumption, in turn, refers to relying on the method of the capability of foreseeing probable and possible threats and risks. Unknown risk is not part of the toolset a risk analyst has and that makes it the ideal foresight for a risk analyst. Beneficial would be to have risk assumptions from other risk models introduced, specially designed for IT under the consideration of the unique aspect of the field (Fenz et al., 2012).

2.2.4.1 Assets analysing method

A Risk Analysis Method and a Management Method (CRAMM) by Central Computer and Telecommunications Agency (CCTA) developed in the UK in 1985, focuses on technical security aspects and comprises asset identification and valuation, threat and vulnerability assessment, and countermeasure selection and recommendation. In the phase of the asset identification and valuation of physical assets, issues to consider are replacement costs, whereas intangible assets, (data and software), are rated as costs occurring if the information would be destroyed, disclosed, or modified.
Based on identified assets threats, vulnerabilities are selected. Furthermore, threats and vulnerabilities and their frequency are estimated qualitatively. For the final risk value, a risk matrix is used to combine asset-specific threats and vulnerabilities information. The advantage of CRAMM methodology is the strong tool support. The support will automatically recommend a suitable countermeasure for a present asset/threat/vulnerability/risk combination when demand for risk mitigation occurs. CRAMM is in general developed for larger organizations, however, a demand for substantial expert knowledge to conduct the complete process of information security risk management adequately (Fenz et al. 2012).

2.2.5 A model of managing information security risks

The model of Bojanc & Jerman- Blažič (2013), is chosen as one of the example models for this research as it is well presented. The model indicates the process of how to identify vulnerabilities and threats against those vulnerabilities.

2.2.5.1 Identify and measure the risk

Bojanc & Jerman- Blažič created a model to effectively manage information security risks. Their model consists of four phases. The first phase is *a risk assessment*. In the first phase vulnerabilities and threats are identified for each information asset. The probability of an incident and loss due to the security information is calculated.
The second phase of the model is *risk treatment*, where appropriate treatment for each assessed risk is selected. Next, the third phase of the model entails *selecting security measures and their effect on risk reduction*. Finally, the last phase of the model includes *the comparison of the selected security measures and an economic analysis of the profitability of each measure*. The whole model in one figure is in the last part of this chapter (Figure 5).

The object of the first phase, i.e. the risk assessment, requires a company to identify and measure its risks. Time obtaining relevant information for the decision-making process is executed in the same measures as identifying risk measures. To be able to measure risks, the company must have useful knowledge of company's information assets. Furthermore, the assessment requires knowledge concerning the assets that might be exposed to threats and the system vulnerabilities where threats might occur. The risk assessment process entails the determination of potential harm to individual risk and the likelihood of what could occur. The model is based on business processes supported by information assets. While there are several business processes in the organization, the model by Bojanc & Jerman- Blažič (2013), focuses only on the core business processes. The risk assessment procedure identifies and evaluates vulnerabilities and threats for every information asset which is part of the business process. The output data of the risk assessment is a risk parameter defined by the probability of occurrence of a security incident and the consequence of that incident.

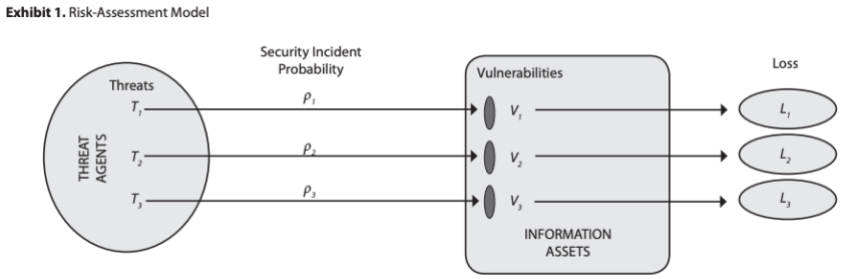

Figure 1. Risk- assessment Model by Bojanc & Jerman- Blažič, 2013.

Bojanc & Jerman- Blažič (2013), made a schematic diagram of parameters for the risk assessment, as illustrated above in Figure 1. T is a symbol of possible threats which have an effect on information systems. Possible threats attack vulnerabilities (v) of information assets. The successful attack creates a security incident (ρ) which presents a final loss (L) (Bojanc & Jerman- Blažič, 2013).

The evaluation of the probability of threats is dependent on factors such as, *what value information brings to the attacker to have an organization's information assets, which resources are available to the attacker, is information security available for the attacker*, and several other required considerations factors. The threat's effectiveness is determined by the vulnerabilities of an information asset. Threats can exploit the

vulnerabilities of information assets. Vulnerabilities can be defined as a weakness or control of an asset exploited by a threat and can be described as an increase in the likelihood of a successful attack on a system, e.g. a threat is leaving a laptop in an unlocked office. The presence of threats, and vulnerabilities are the ones affecting the probability of the laptop being stolen. Vulnerability cannot cause a loss. A condition is allowing a threat to impact information assets. In the model of risk assessment by Bojanc & Jerman- Blažič, the connection between vulnerability and threats is displayed linearly to improve the clarity of the diagram (Figure 1.). The model supports the existence of multiplied vulnerability-threat relations. One threat may attack a single vulnerability or multiple vulnerabilities and multiple threats may attack a single vulnerability

Threats to a company can be tangible or intangible. Every company has to identify the threats and the vulnerabilities to be able to avoid them. The identification of both, intangible and tangible threats is necessary for the company to be successful in the future. ISO 27005 (2008) "Information Security Risk Management" standard classifies threats into the following categories:

- Physical damage: fire, pollution, dust, corrosion, destruction of equipment or media, etc.
- Natural events: seismic phenomenon, volcanic phenomenon, floods, etc.
- Loss of essential services: the failure of air-conditioning, failure of the water supply system, loss of the power supply system, failure of telecommunications equipment, etc.
- Disturbance due to radiation: electromagnetic radiation, thermal radiation, etc.
- Compromise of information: the eavesdropping, theft of media or documents, disclosure, the retrieval of recycled or discarded media, etc.
- Technical failures: equipment failure, a saturation of the information system, etc.
- Unauthorized actions: the unauthorized use of equipment, fraudulent copying of software, the corruption of data, illegal processing of data, etc.
- Compromise of functions: error in use, abuse of rights, the denial of actions, etc. (Bojanc & Jerman- Blažič, 2013)

2.2.5.2 Choosing the right strategy

The second phase of the model is the *risk treatment*, where appropriate treatment for each assessed risk is selected. The organization can choose from several risk reduction strategies. For minimizing the risk, the organization must choose the right risk reduction strategy (Figure 2.)

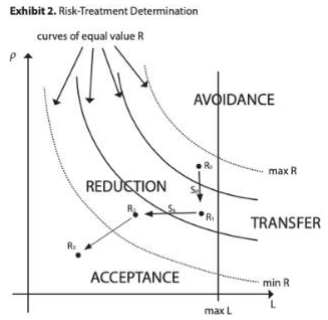

Figure 2. Risk- Treatment Determination by Bojanc & Jerman- Blažič, 2013.

In line with Figure 2, there are at least the following a few options of basic risk management for an organization to choose from:

- Reduction of the security risk by implementing appropriate technologies and tools (firewalls, antivirus systems, etc.) or adopting appropriate security policies (passwords, access control, port blocking). As a result, the probability of a security incident reduces or limits the loss caused by the incident. The reduction is primarily a risk-management strategy.
- Transfer of the security risk by either outsourcing security service provision bodies or an insurance agency. This method of transferring the risk is becoming an increasingly important strategy for applying security measures within an organization.
- Avoidance of the security risk by eliminating the source of the risk or the asset's exposure to the risk. This is usually applied in cases when the severity of the impact of the risk outweighs the benefit which is gained from having or using a particular asset, e.g., full open connectivity to the Internet. An engineering manager selects risk avoidance as and the organization terminates some activities, even though it protects them against the risk that would have consequences that are considered serious.
- Acceptance of the security risk as a part of business operations. Risk acceptance is a reasonable strategy for risks where the cost of the investment or insuring

against the risk would be greater over time than the total losses sustained (Bojanc & Jerman- Blažič, 2013)

2.2.5.3 Selecting security measures

The third phase is *selecting security measures, and the effect they have on risk reduction*. Determining a line between each treatment can be challenging, as the line can be understood from different perspectives. A firewall can be noticed as risk avoidance or risk reduction if the company renounces the benefits of open networks to avoid the risk. When choosing the treatment for a particular risk, the determination of whether to employ a compromise and combine two options has to be decided (Bojanc & Jerman- Blažič, 2013).

A combination of treatments is possible when a chance to choose between several options exists. Thus, a company can initially reduce the risk with investment and transfer the remaining risk to an insurance agency or assess the remaining risk to be acceptable, thus introducing no additional measures. The purpose of security measures is to help the company to prevent or reduce the damage caused by the realization of one or more threats. Such measures can be, such as using software, organization policies, physical protection, algorithms, and several others. The appropriate selection of security measures is essential to ensure effective information security (Bojanc & Jerman- Blažič, 2013).

Integrating security measures into the model (Figure 3.) illustrates how companies can make security measures for everyone's use, and thus makes risk management available to all the employees, such measures are prevention, detection, awareness, control, and recovery (Bojanc & Jerman- Blažič, 2013).

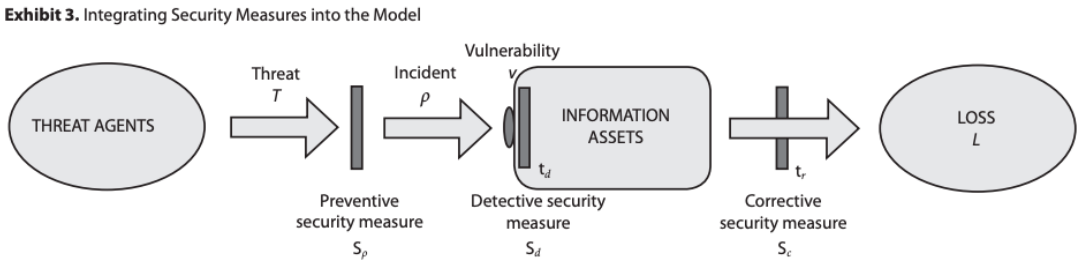

Figure 3. Integrating security measures into the model by Bojanc & Jerman- Blažič, 2013.

2.2.5.4 Comparison of selected security measures

The last part of the model is *the comparison of the selected security measures and an economic analysis of the profitability of each measure*. The interest in information security is rapidly growing and companies are more aware of security issues. Furthermore, companies consider security as one of the basic elements of any information system. However, a fully secure system does not exist and therefore the organization should choose the security level which is acceptable for it (Bojanc & Jerman- Blažič, 2013).

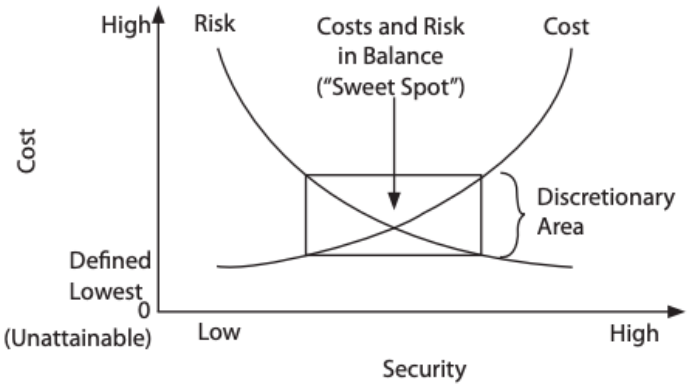

Figure 4. Balancing Cost and Security by Bojanc & Jerman- Blažič, 2013.

Determining an appropriate security level is not easy. The model by Bojanc & Jerman-Blažič (2013), in phase four presents the balance between cost and risk (Figure 4.). The basic idea of risk management strategy is to reduce the risk with the appropriate technologies, tools, or procedures. Reducing risks will reduce the probability of a security incident or damages caused by the incident. The organizations which are involved in the process of electronic commerce should invest in measures related to information security (Bojanc & Jerman- Blažič, 2013).

The idea of the Bojanc & Jerman-Blažič (2013) model can be observed below (Figure 5.), the main idea of the model is to initially be aware of threats and vulnerabilities and then think of the security level which is demanded to prevent the risks from occurring. Either risk reduction or risk transfer is the strategy that the company has chosen. With the balance between cost and security, mandatory actions are implemented. In principle, a company should have the resources to apply security measures in line whit the mandatory level. The balance between cost and security is one of the most important

factors for a company. The model is approving changes as vulnerabilities and threats are changing with time and technology evolving. A company is thus required to review its vulnerabilities and threats often to make sure the security measures are up to date security.

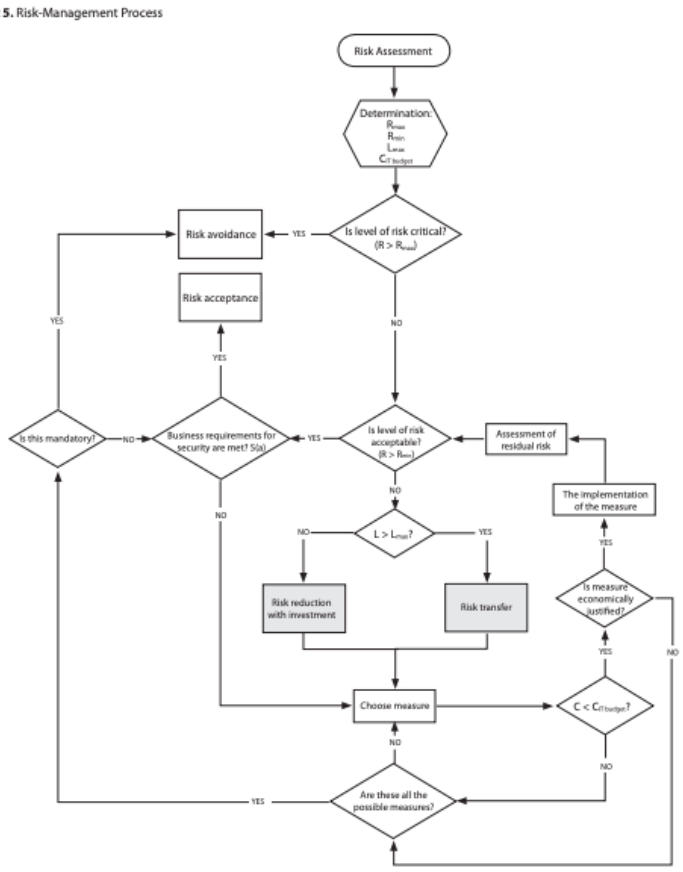

Figure 5. Risk management process by Bojanc & Jerman- Blažič, 2013.

2.2.6 Information security risk management in general

The model of the risk management process by Bojanc & Jerman- Blažič (2013), is only one model of risk management. However, also other models exist and, they follow almost the same procedure. In general, the aim for the model is the same, i.e. identifying risk and vulnerabilities to be capable of void threats.

Information security risk management methodologies have only minor differences among themselves. In general, every one of the methodologies requires inventory and security classification of relevant infrastructure elements and identification of the organizations' missions and goals in the initial phase. From a high-level perspective, subsequent phases typically required the identification of threats and corresponding

vulnerabilities to determine threat probability together with implemented controls. Identification of threats is required when threats are used in combination with results. Impact analysis is created to determine actual risks, thus considered circumstances methodologies in the analysis share several commonalities and a few differences. Differences create generic information security risk management, which represents the considered methodologies from a high-level perspective. Such perspectives are system characterization, which is the definition of the system boundaries and assets used or required by the defined system inventory of tangible and intangible assets, and the determination of the acceptable risk level for each inventoried asset. The threat and vulnerability assessment requires the determination of potential threats, corresponding to the threat origins, and vulnerabilities (Fenz et al., 2012).

A security requirement checklist is necessary, as a checklist can be used for a compliance evaluation regarding current or planned controls for the subsequent risk determination. Risk determination determines among others the probability of a threat exploiting certain vulnerabilities in the present system. The subsequent impact analysis determines the impact on an organization's ability to perform the company's mission if a threat should successfully exploit certain vulnerability. Control identification is elaboration by considering implemented controls, on additional control implementations which could mitigate or reduce risk to an acceptable level. Control evaluation and implementation evaluate the identified control implementations or combinations regarding their cost and benefit ratio. The controls are selected to be suitable for mitigating the risk to an acceptable level at the lowest possible costs are incorporated in the control implementation plan (Fenz et al., 2012).

2.2.6.1 Annual standard of useful practice

An annual standard of useful practice is annually published by the Information Security Forum (ISF). The annual standard provides high-level guidelines for information security, including the standard of distinguished environments. The guidelines offer a particular set to enterprise-wide security management, critical business applications, computer installation, networks, and system development. A broad spectrum of information security arrangements is required to preserve the business risks at an acceptable level (Fenz et al., 2012).

2.2.6.2 Information Risk Analysis Methodology

Another model, referred to as Information Risk Analysis Methodology (IRAM) mainly focuses on the reduction of risk impact, management of threats and countermeasures, and legal or regulatory compliance. The methodology consists of three stages, starting with business impact assessment, where crucial elements and applications to the business process are identified and the criticality concerning confidentiality, availability, and integrity is determined. The second stage entails threat and vulnerability assessment, where threats to prior business-critical assets and exploited vulnerabilities are identified. Control selection is the third phase where controls provided by the standard of useful practice and capable of mitigating potential exploits and threats are determined. The last phase is based on control's effectiveness as a threat countermeasure, thus ignoring the cost efficiency aspect of decision support (Fenz et al., 2012).

2.2.6.3 Generic Methodology

In the research conducted by Fenz et al. (2012), the definition of generic methodology refers to large information security risk management. This methodology allows aligning problem and solution identification to the generic phases of methodology which ensure that research results can be applied to a broad range of existing information security risk management methodologies. Simplifying the assessment of risk is an exciting trend at the moment. Using simple risk models creates an impact on the information security approach, thus companies have easier access to manage the threats and vulnerabilities. Furthermore, the model with a simple risk allows easy and fast risk assessment, which can be applied to inexperienced personnel, however, some inaccuracy results from the simplicity. Some models can notice the similarity in their generic nature. Many models can be considered similar due to their generic nature. Models focus on the technical threats and vulnerabilities of the IT sector. However, at the same time, risk management originated in the financial sector and is managed with security risk management.

The establishments of risk management are basic security elements ISO 15408, 2008, listing assets, the owner of the assets, threats, vulnerabilities, risks, and measures. The owner who places value on the assets is responsible for safeguarding them. The owner must analyse the potential threat to determine which ones apply to the environment, and which of the results are at risk. The analysis can assist in the selection of

countermeasures to reduce vulnerabilities, counter risk and reduce risk to an acceptable level (Bojanc & Jerman- Blažič, 2013).

2.2.7 Differences between management positions

Some companies do not have any personnel responsible for information security. Similarly, where in smaller companies, the employee responsible for information security might have other responsibilities to handle simultaneously whereas larger companies have a whole department for information security. In general, the information security manager is in charge of the issues related to information security. Some information security policies are mandatory for companies. Such policies are created after the increased use of the internet and instant messages. To ensure the compliance of the policies in use, a company has to have the necessary technical security measures (Von Solms, 2006).

Information Security Governance has two aspects. On the one hand, it entails policies and procedures and on the other hand, it includes the compliance and enforcement of such policies and procedures. According to Von Solms (2006) "Information Security Governance consists of the management commitment and leadership, organizational structures, user awareness, and commitment, policies, procedures, processes, technologies, and compliance enforcement mechanisms, all working together to ensure the confidentiality, integrity, and availability (CIA) of the company's electronic assets (data, information, software, hardware, employees, etc.) are maintained all the times". Information security management, however, covers only part of the more extensive aspect of information security governance. The definition of information security management covers aspects related to operational information security management, such as the creation of policies, and procedures. One aspect is the missing compliance monitoring and enforcement in the traditional role of information security management that is required by information security governance. The traditional role of information security management has changed in the last couple of years with the aspects mentioned above (Von Solms, 2006).

The difference between information security management and information security operational management is specified. According to Von Solms' (2006) research, the difference has typically existed thus it has not been as clear and determined as it is

today. Von Solms also continues that the difference has become essential to information security governance, and in the future the separations between these two are necessary. Information security operational management used to be a part of operational management, as today the role has more activities. Requirements to be noticed as a part of information security governance were essential. Today, information security governance-related activities include, thus are not limited, to logical access management, firewall management in terms of setting its rights, virus and malicious software management, and setting and updating security settings and configurations of workstations and servers, among several other tasks. The tasks are executed to make sure the IT environment is set up to fight against any risks which may affect confidentiality, integrity, and availability. Traditionally, tasks have been recognized as information security managements issue, as the task is recognized as a technical task it is ideally executed by a technician. However, in today's business life the image has been changed and non-technical activities in information security management have found their rightful place. Non-technical activities include activities such as the creation of information security policies and procedures, compliance enforcement mechanisms to ensure compliance with all policies and procedures are enforced, with several more tasks.

2.2.7.1 IT and corporate governance strategies

Useful IT and corporate governance strategies demand that risks should be lowered and managed properly. The essential part of risk mediation is to enforce compliance measurements and enforcements, which have become an important component of general IT risk management. A company requires to have a management information security strategy for the day-to-day compliance measurement and enforcement of activities which has grown the field of management information security governance. Often management information security is in an outsourced, however, activities are monitored in real-time, and issues are reported without delays to those whose take relevant action (Von Solms, 2006).

A proper information security compliance program should not be part of the information security operational program to report being objective. If the operational information security department is required to measure how well a company can comply with relevant policies and procedures, and how successful the company's risk mediation

effort is, the results may otherwise not be as objective or true as they could be. The separation between these two departments is an important aspect of useful IT governance (Von Solms, 2006).

An IT-management risk profile could typically be a requirement for actions. The information exists for all levels of risk compliance and exposure. The frameworks of what the IT risks are, on what level should they be managed, at what level they are accepted or transferred, and to what level executive management accepts these risks, are required. The IT-management risk profile has multiple approaches to be created. Management of the profile is created in real-time IT risk compliance profiles reflecting the level of management of IT risks (Von Solms, 2006).

2.2.7.2 Security department

Regardless of the company's business field, one of the most important roles of the security department is protecting the company's assets, equipment, product or merchandise, reputation, and employees. This responsibility also extends to non-employees, meaning guests or customers. The security department is required to prevent all losses. The prevention is executed with strategies and philosophy to deny the criminal opportunity to succeed (Sennewald & Baillie, 2016).

The company executive security director is selected by the company managers. The security director is a member of the management team. However, the director should not be viewed as only a security specialist though rather as an effective executive in the security field. The security officers must not have a reputation as company police, yet rather as important members of the company security. More requirements become for security departments and security head directors when the company grows. In general, the security department should indicate one person responsible for and managing the department (Sennewald & Baillie, 2016).

When security departments and managers are choosing to mitigate risks, they will choose one or more different styles of control. The types of controls include such as administrative, logical, physical, and many more. Administrative controls or procedural controls consist of written policies, procedures, standards, and guidelines that form the framework for running the business and managing others. Other types of administrative

controls such as password policy, hiring policy, and disciplinary policies are created by government and corporate security policy. Based on the administrative controls, logical and physical controls are chosen. Logical controls or technical controls are the use of software and data to monitor and control access to information and computing systems, e.g. passwords and firewalls. Physical control refers to, such as monitors, and controls concerning the environment in the workplace and computing facilities. Administrative controls concern the access to and from such facilities, including doors, locks and smoke, and fire alarms (Sattarova & Tao-Hoon, 2007).

2.3 The role of the CEO in a company

The role of a CEO and how much leadership is needed are highly based on the size of the company. In smaller companies, the CEO's role is more critical and requires closer involvement in daily matters, trusting, and personal working relations with employees. When a company increases in size, its managerial structure is often formed by the furthering owner. Furthermore, the potential for the control role of directors in support of the CEO tends to increase. In SMEs, it is common to seek external expertise when none of its personnel is equipped with some particular knowledge. External expertise can include training that enables a person in the company to perform a certain task in the future. Companies with many managers often have a higher level of managerial education development as opposed to owner/proprietor management (SMEs) (Bennet & Robson, 2004).

A CEO's main task is to be in charge of the funds of the company. Funds in this context are understood as anything that limits resources within any organization. A CEO's task is to weigh the costs of a data breach and the costs of other initiatives and determine the level to be spent on information security. Companies today, are in general likely to spend more resources on information security after being subject to a cyber incident. This is understandable, as, without incidents occurring, a question will arise whether there is a demand for information security. Consequently, companies use their funds for something other than information security. Usually, information security is viewed as more of a cost for the business as it does not produce increased revenues or reduce costs for the organization. Thus, security investments are the choice of a CEO, not an absolute matter. Information technology and security provide support to the business

and exist as a result of that relationship. The business vision and mission must drive projects forward. However, companies should not forget the risk profile and investments that are also required for the project to succeed (Fitzgerald, 2007).

A CEO is considered a person who can control the whole organization. A CEO is expected to support the security department's initiatives, as they relate to the mission of the business (the so-called equal support). Furthermore, a CEO must ensure that ongoing security operations are provided with the necessary funding. A CEO is accountable for holding the components of the business and securely achieving the company's objectives. The responsibility of a CEO towards security is not different from responsibility towards any other part of the business. A CEO is continuously concerned with financial, operational, and business risk decisions. A CEO will have all information to make the decision based on facts that will not expose the organization to a regulatory compliance issue, which may create a risk to the business reputation or decrease the efficiency and effectiveness of the organization's capability to produce. When launching a new product or service, a CEO must have a clear understanding about the security risks relating to the launch. Otherwise, the unclear security risks might affect the launching and appear to create lack of control for a compan (Fitzgerald, 2007).

2.3.1 Imperial CEO

An imperial CEO is an individual who wears multiple hats, one in the role of the public company chairman and another in the role of the CEO of the same company. The role of a chairman of the board is to lead the members of the board of directors, whereas, for a CEO, the role is on general corporate oversight. A CEO has fiduciary responsibility for selecting new members for the board of directors, setting executive compensation, evaluating executive performance, and through the audit committee, evaluating the company's financial status and disclosures on behalf of shareholders. Having a "double" role creates conflict with the idea of the CEO being the subject of board discussion and at the same time the head of the board. The double role can affect the decision on matters such as who joins the board, management teams performance, and compensation of the board (Green, 2004).

A CEO who has unfettered the control of the board can create benefits by working only for him/herself and not for the shareholders. All CEOs do not take advantage of the situation and advance their position. In general, a CEO wants to make decisions that benefit the company. Conflict of interest in the CEO's position can have severe criminal consequences. Furthermore, conflicts of interest can be disastrous if they are not checked. The majority of the companies are aware that the conflict acting in both of the roles can create a negative impact. Despite these, imperial CEOs are common in public companies in some countries. These countries seem to think it would be disruptive to demand a separation between the board of directors and the CEO. In the US, around 80% of the companies have imperial CEOs and in France, the percentage is even higher. Nevertheless, from the FTSE 350 companies, globally 95% of the companies split the duties between the board and the CEO. Germany and Netherlands have executed the split by board structure. A non-executive supervisory board exerts general oversight and governance rights, and a management board consisting of company executives provides operational supervision. The structure, by its definition, precludes the creation of imperial CEOs (Green, 2004).

If the imperial CEO is the used model in multiple countries, the company should work with another structure. However, the main reason for the situation not being changed is that the imperial CEOs do not resign from his/hers positions. Furthermore, imperial CEOs have been presented the power and boards are unwilling to upset the CEO. Being the chairman of the board is considered the highest recognition and the CEO may think that s/he has worked hard to achieve it. Moreover, some think that separating these roles will not ensure useful operating performance. It can be contested whether a qualified chairman is found and whether any benefits it brings to a company are short-resided, as the director's independent mind degrades the longer s/he is in the role. In time the CEO begins to identify him/herself with some decisions previously made (Green, 2004).

2.3.2 The reputation of the CEO

A CEO plays one of the most important roles in the company, whether it is an internal or external audience evaluating the CEO. The reputation of a CEO is based on almost every activity in a company, such as a stock transaction, a response to a crisis, or the creation of a best-in-the-industry talent pool. Shareholders focus more on the CEOs than before, as a CEO with a great reputation has multiple positive effects on the company.

Thus, a CEO's reputation can be one of the most powerful tools used to create shareholders' value, wins support during times of crisis, and help attract and retain the ideal and brightest employees (Gaines-Ross, 2000).

According to Gaines-Ross (2000), seven qualities maximize the reputation of a CEO. The first one is a CEO's awareness of the company's visions and values, which can be viewed through the eyes of the employees, shareholders, and customers. The second quality is a CEO realizing the company is discoverable to others and the company ensures that the company is viewed in a positive light and as a place where everyone desires to work. Communication is the third quality, which represents that a CEO must bring the vision and the strategy in an understandable aspect to both internal and external partners. The fourth quality is for a CEO to understand both a word-of-a-mouth and online talk and to deliver these comments clearly to the stakeholders. The fifth quality is that a CEO can lead a strong management team. Having leadership skills is one of the most important qualities, and revealing these great leadership skills to external parties affects positively the CEO's reputation. The sixth quality is that a CEO is determined in decision-making and risk-taking. A CEO must understand and consider how the actions are executed, and how they affect competitor businesses. The seventh and the last quality is that a CEO understands what knowledge stakeholders demand and delivers this information personally and with confidence. One of the most important qualities of a CEO is to adapt to changes, as they are inevitable. When the adaptation is well-executed, it will affect the shareholders and the employees of the company.

Communicating through several channels creates a CEO requirement in today's world to handle and perform in many of the channels to bring value to shareholders, employees, and extended parties. Communicating through several channels, usually remotely, is easier with today's technology and it creates new opportunities and working guidelines on an increased tempo. As Gaines-Ross (2000) wrote, a CEO can be considered as a helm who is visible and can create a positive aura around themselves. Thus, the companies whose CEO is the champion can make all the difference between success and failure.

2.4 Summary of the literature review

The literature review used in this research is a theoretical framework for the interviews executed with the respondents. The literature review consists of three parts which are information security, corporate risk management, and the role of the CEO. Subjects are reviewed from a general perspective and the point of view of the CEO.

The chapter on information security elaborates on how the phenomenon has changed during the past few years and how the importance of information security will be increasing in the future. The main types of cyberattacks for a company can be divided into inside threats and outside threats. For the attacker, it is more cost-effective to attack from the inside rather than order an attack to be performed from outside the company. The inside attack is an attack executed by someone who has access to the company's data and who possesses important information that can be taken advantage of.

In the chapter concerning corporate risk management, several models are presented. Such risk management models can be used for identifying threats to the company's vulnerabilities. One of the models, created by Bojanc & Jerman- Blažič (2013), is presented in more detail in the literature review. After identifying the threats and vulnerabilities, the decision has to be made on what scale will be the management of the risk. Although only one model is presented in this research, several similar models exist. The main purpose of all the models is to have risk management at a low cost by offering protection on a scale that is secure enough for the company.

The last chapter in the literature review is about the role of a CEO. The position of a CEO changes with the size of a company and with the nature of a CEO. An imperial CEO is an acting CEO and the head of the board of directors simultaneously. This position can be doubted as a CEO will have numerous decisions to consider when acting in both roles, and s/he wears two hats creating a risk of conflict of interest in decision-making. Finally, the reputation of the CEO will determine the success of the company as in numerous cases the CEO is considered as the face of the company.

3 RESEARCH DESIGN AND METHODOLOGY

Chapter 3 presents the used methods of the research with the sampling method of the respondents for the research and the strategy applied for analysing the responses. The used theory is presented and how these theories are used in this research.

3.1 Research methods

The research method of this master's thesis is the qualitative research method. In addition to the qualitative method, quantitative and mixed methods are presented to understand the differences in these methods. The theory in this research is grounded theory, which is initially based on the literature review and empirical data. The theory provides room for reflection during the analysis. Lastly, the method of exploratory research is used to work in writing the literature review and conducting the interviews. Conclusions are formed based on the literature review and interview findings, hence empirical data. A sampling method presents the characteristics of respondents and why they were selected.

3.1.1 Different research methods

Research methods are selected and applied to review the problem and the research questions from a certain viewpoint that the researcher has decided to look into. A single approach or combination of two methods is the most commonly used method for conducting research. The researcher must decide the study method that enables the researcher to receive the research aims and goals (Adams et al., 2007). Three main types to assess the data are qualitative research methods, quantitative methods, and mixed methods. Qualitative methods are used to explore and obtain a depth understanding about the reasons behind certain questions or phenomena, while qualitative methods are used to test and confirm hypotheses based on an existing conceptual model and obtain a breadth of understanding of the predictors of successful implementation. Each methodology has different expectations and standards for determining the number of participants or reach of data that is required to achieve the aims of the research. A mixed methodology design is a combination of both of the main research methods. Mixed designs are viewed preferably in implementation research because they provide a

better understanding about research issues together rather than either qualitative or quantitative approaches alone would (Palinkas et al. 2013).

3.1.1.1 Quantitative method

Quantitative methods place the primary emphasis on generalizability. The method seeks to ensure the knowledge gained by the representative of the population from which the sample was drawn. The method relies on establishing formulae for avoiding Types I and Type II errors with the selected number of participants, (Palinkas et al. 2013, 533). Quantitative research is usually based on the methodological principles of positivism and neopositivist and adheres to the standards of a strict research design developed before the actual research. The method relies on quantitative measurement, hence statistical analysis only. The quantitative research method is widely used in almost every sphere of life (Adams et al., 2007).

3.1.1.2 Qualitative method

The qualitative method sets primary emphasis on saturation which is obtaining a comprehensive understanding by continuing to sample until no new substantive information is required. The method often relies on precedents for determining the number of participants based on the analysis process, such as, the phenomenology study includes multiple interviews with 3-6 participants versus grounded theory includes one interview with 20-30 participants (Palinkas et al., 2013). Qualitative research uses some methodological approaches based on diverse theoretical principles such as Phenomenology, Hermeneutics, and Social Interactionism. In this type of research, data are collected and analysed in a non-quantitative type, and the aim is more on an exploration of social relations, describing reality as it is experienced by the respondent (Adams et al., 2007).

The chosen method for this research is qualitative research. With qualitative research, there is a chance to ask extra questions to receive a better insight into the responses. The interviewers were asked to respond to the question as to how they think about the issue in question. As all the respondents were CEOs, the respondents gave a great insight into the ideas of the CEOs.

3.1.2 The Interview style

An interview is one of the most common styles of collecting data for research. Interviews are time-consuming, however, they are useful because of their flexibility. With an interview style, there are numerous forms with the consistency between in-depth follow-up questions, and guided conversations to highly structured questionnaires. Questionnaires are often used to elicit attitudes and perceptions although they can be a source of factual information (Guthrie, 2010). The research type used in this study is semi-structured. Three types of interview styles exist: unstructured, structured, and semi-structured. Only the semi-structured style is presented in more detail as it is used in this study.

3.1.2.1 Structure of the interview

Using semi-structured interviews indicates that the interviews are directly comparable with each other. Interview instructions usually entail a standard introduction and conclusion, however flexibility provides the order of questions a natural flow for further discussion. Furthermore, semi-structured interviews usually provide coded closed-response questions with the opportunity to follow up with open-ended questions. Using this style will help the interviewer to receive a better understanding about the respondents' views. The result is a combination of quantitative and qualitative data, and in this research, the responses are analysed with the qualitative method, as they are compared with each other, which creates the quantitative approach. Usually, interviews are executed one-on-one, even though, it is also possible to conduct a group interview. One of the most common types of respondents in a semi-structured interview is to use a focus group which is a semi-structured technique derived from marketing and advertising (Guthrie, 2010). According to Saunders et al. (2007), semi-structured research is another name for qualitative research interviews. The interviewer can request more questions from the respondent if a need arises.

For this research, the semi-structured interview was selected as the research is a qualitative research method, and the best understanding about the respondents is collected with a semi-structured interview style. The style functions more freely than a structured interview, thus there is a structure that the interviewer can follow, and can also ask extra and follow-up questions. The style functioned for all the respondents as

some of them were asked multiple follow-up questions and with some others, the interview was more based on a ready-made structure with fewer follow-up questions.

3.2 Sampling method

The sampling method used to choose the right participants for the research is purposive sampling. Purposive sampling is one of the most commonly used methods in qualitative research. In purposive sampling, the choice of participants is made by the interviewer. Therefore, the demand for certain underlying theories or a certain number of participants does not exist. The researcher decides which information is demanded and on that basis searches for the participants who are qualified and willing to provide the information based on their knowledge or experience. It is advisable to let the participant know what the phenomenon is that is being researched and look into their willingness to participate. The characteristics of the purposive sampling used in this research can be viewed below (table 1.). By using purposive sampling, the researcher confirms the participants are relevant to the research. Purposive sampling methods place primary emphasis on saturation, e.g. attaining a comprehensive understanding by continuing to sample until no new substantive information is acquired (Etikan et al., 2015). A researcher is not allowed to generalise a population with purposive sampling. Purposive sampling is not a random sample or a convenience sample (Bryman & Bell, 2011).

The characteristics used in this research are:

Table 1. The characteristics of the participants

CEO of the company
Finnish based company
small/medium-sized company
IT-company

Whether the methodology used is quantitative or qualitative, sampling methods are intended to maximize efficiency and validity. Sampling must be consistent with the aims and assumptions inherent in the use of either method (Palinkas et al., 2013).

The challenges of using a purposeful sampling strategy are, such as that the range of variation in a sample of which a purposive sample is to be taken is often not known outside of a study. The saturation is determined by a priory based on an existing theory or conceptual framework, or it may emerge from the data themselves, which is called a grounded theory. Furthermore, there may be a challenge in terms of a difference in opinion about these approaches among qualitative researchers. Some researchers resist or refuse systematic sampling of any kind and reject the limiting nature of such a realistic, systematic, or positive approach. In quantitative research, the participant in an interview must be selected rationally to gain the aims of the study and it is conducted with purposeful sampling, not systematic (Palinkas et al., 2013).

3.3 Data collection

The six selected CEOs were interviewed for the research of this master's thesis. The companies were searched by using the characteristics presented above (table 1.). Accordingly, the characteristics of the selected companies were small-sized Finnish IT-companies, with the field of business being IT. The companies were found by internet search, and the CEOs were contacted personally via LinkedIn by asking if they were interested participating in the research. The interviews were executed via Zoom where both, the interviewer and the participant were free to conduct the interview anywhere they pleased. All the interviews were conducted during November and December 2021.

Before interviews, the respondents were sent a message either through LinkedIn or email. The message contained the main ideas of the interview, the time frame, and the rights of the respondents. The company names were left out from the research as the interview was anonymous. The respondents were also told that the interview will be recorded via Zoom.

All the interviews were between 25 and 45 minutes and were audio recorded and then transcribed verbatim for the analysis. The respondents were asked to respond as to how they think about the subject and freely offers examples and future recommendations.

3.3.1 The respondents

The list below (table 2.) presents the participated companies by the field of study and by the number of employees. The names of the companies are left out as the interviews were anonymous and their names have been replaced with the letters from A to E.

Table 2. List of the participating companies

The company	**Field of business**	**Number of employees**
Company A	*Software as a service*	*1 + 15-20*
Company B	*Software as a service*	*44*
Company C	*Clouds & colocation*	*40*
Company D	*Consulting & Google workspace service*	*40*
Company F	*Logistic & Information technology*	*40*
Company E	*Software as a service*	*30*

All the companies were small size companies working in different fields in the IT sector. Three out of six companies were developing software as a service (SaaS). Company D specializes in the Google Clouds service and offers services to help other companies to use Google Cloud services. Company C's business relates to offering a cloud environment and colocation.

The size of the company in the sampling method was small/medium. While searching for the participants, the invites for the interview were sent also to medium-sized companies. Unfortunately, there were no CEOs from medium-sized companies participating. The interviewed CEOs were all from small-sized companies. Interviewing only small-sized companies' CEOs ruled out the medium-sized CEOs' perspective from these responses.

3.4 Selected theories

The selected theories for this master's thesis are exploratory research and Grounded theory. These two theories were selected because they offer space for changes in the responses and the analysed data can change the becoming theory. Both the theories search for responses to some ongoing situations and are aiming to gain knowledge of the situation in a new light.

For this research, there is the theoretical framework and collected empirical data. In the analysis part, they were continuously linked together which is why exploratory research and Grounded theory were selected. The grounded theory adds the coding of the responses which creates the comparative effect for the responses.

3.4.1 Exploratory research

In exploratory research, three research designs exist that the researcher can conduct research with. Exploratory research indicates the researcher to discover what the ongoing situation is with the subject of interest. The researcher gains insights and presents the phenomenom in a new light. Using exploratory research is useful when the researcher is searching for clarification and understanding about the problem of the research. In exploratory research, three principal acts of conducting the research exist:

- A search of literature
- Interviewing 'experts' in the subjects
- Conducting focus group interviews

In the research of this master's thesis, two out of three principles were used: a search of the literature and interviewing 'experts' in the subject. Using these two methods gave the advantage to the interviews being flexible and adaptable to change. Using exploratory research indicates the researcher must be willing to change the directions of the results with the new data which might appear during the research, and this might bring new insights to the results. Exploratory research does not indicate the absence of the direction to the inquiry. The focus is initially broad and becomes progressively narrower with the research progress (Saunders et al., 2007).

3.4.2 Grounded theory

Grounded theory has become one of the most used theories for analysing qualitative data. Grounded theory is a method where no actual theory exists, to begin with, as the theory is created from the research results. With the results, certain themes and issues will arise from the responses. The data will be analysed as collected from the responses and a conceptual framework will be created. Consequently, a research purpose will exist, to begin with. In this research, the purpose is created during collecting the literature review and the clear purpose arises from combining the theoretical framework with empirical data. The purpose is built around the core or central theme of the collected data. Referencing academic publication is often part of the tactic of persuading the readers of the legitimacy of one's research and this process can be discerned in the citation of grounded theory.
With the grounded theory, not as much attention is demanded of the nature of procedures outlined. Already produced reports do not exist. Those reports could be sufficiently rigorous for a researcher to seek in advance of their research. Grounded theory can be observed as more than a strategy than a set of procedures (Saunders et al., 2007).

The data analysed in grounded theory are divided into units called open coding. Recognizing the relationship between categories is called axial coding. The last division is selective coding, where the categories produce a theory. The sampling of the respondents in the grounded theory used is purposive (Bryman & Bell, 2011). Grounded theory is the method used in the research of this master's thesis. The method was selected because a grounded theory has no theory, to begin with. The theory will be created from the literature review and the participants' responses as it is conducted in this research. There is room for changes during analysis as the results may change with the participants' responses. The responses are collected together and then put into different categories. After categorizing the main ideas for a theory, the most important ideas are selected, and based on those selections the theory is created. Data collected in grounded theory are usually from one-on-one interviews, focus groups, and participants' observations by the researcher. The main idea of a grounded theory is to discover or generate a theory.

3.5 Analysing the data

According to Creswell (1998), data analysis is not an off-to-self task, it is rather a custom-built revised, and 'choreographed' tool. In qualitative research methods, researchers usually learn by doing. This can be criticized by claiming that qualitative research is largely intuitive, soft, and relativistic or that it reverts to three "I's": insight, intuition, and impression.

3.5.1 Coding

When analysing the data collected with the qualitative research methods, using categorization is one of the most common strategies. Consequently, the responses will be encoded or labelled to examine their similarities. The identifications of the codes will be guided by the purpose of the research and the objectives. The categories must be well-structured and will provide an analytical framework for the analysis. Categories have two aspects, namely the internal aspect, which requires responses to be corresponding with the data, and an external aspect that must correspond with other categories (Saunders et al., 2007).

According to the grounded theory, the initial phase of coding is open coding. Open coding implies that the research begins by categorizing the text for salient categories of information. The second phase is axial coding, which requires identifying a single category from the categories of the open coding as the central phenomena. The third phase is selective coding. In selective coding, the researcher establishes the theory (Creswell, 1998).

For this master's research, the responses of the CEOs were first transcribed to find the extracted phrases and sentences that the respondents used and then used the first coding to categorise them. After the first coding, the second coding, axial coding, was that the extracts were further analysed to understand their significance for this research. In the last part, selective coding, the further analysed responses were reflected in the theoretical framework to create a better understanding and to create a theory for the whole master's research.

3.6 Validity and reliability

Validity measures whether the findings are what they appear to be. Validity can be described as responses being correct, which will make them valid and not something untruthful for the study (Saunders et al. 2007). Validity is also concerned with the accuracy and trustfulness of the research findings (Brink, 1993).

The validity of this research comes from the fact that all the respondents are in CEO positions which refers that the responses can be analysed from the point of view of the CEOs. The interview questions are valid as all the respondents could answer them and there was no subject that they did not feel is their area of business. The interviewed questions were created with the literature review which also creates value for this research.

Reliability is the consistency, stability, and repeatability of the researcher's ability to collect information accurately, and the ability to research the method of yield consistently over the same results over repeating testing (Brink, 1993).

According to Saunders et al. (2007), there may be four different threats to the reliability of the data or the result of the study. These four threats are, firstly, subject or participant error, secondly, subject or participant bias, thirdly, observer error, and lastly observer bias. Hence, the time and place might affect the responses of participants. Furthermore, the observer, i.e. the researcher may express a question in a different approach, which may affect the response.

When using non-standardized research methods, the results must not be intended to be repeated since they reflected the reality at a certain time and place when they were collected (Saunders et al., 2007). As the result, reliability is easier to measure in quantitative research than in qualitative research. Qualitative research should be evaluated according to trustworthiness and authenticity. Measurements of trustworthiness and authenticity are credibility, transferability, dependability, and conformability (Bryman & Bell, 2011).

Reliability in this research is in the responses. The threats to reliability are subject to participant error and observer error. There might be errors in the form of the questions which might create either participants' or observers' errors. There might be differences in the way the questions are presented. On the other hand, according to Bryman & Bell (2011), better measurements for reliability are trustworthiness and transferability and both of these are in the responses of the CEOs. The trustworthiness relies on the fact that all the respondents are in CEO positions, and they are speaking from the experience of a CEO. The transferability relies on the research style. The responses are compared with each other and then reflected in the theoretical framework. The research presents the responses in a certain time and place and in the future they might not be reliable, however, for this master's thesis, they are reliable.

4 RESULTS

The results of participants' responses are categorized using the grounded theory method. Using open coding, axial coding, and selective coding. The focus of the interview is on information security from the perspective of a CEO. The interview entails three parts with different aspects to look into information security. The topics that were discussed with the respondents were information security, risk management, and the role of a CEO. All these three parts are categorized below, including a summary of the main points of the responses.

The first category is where the responses of the CEOs are categorized to understand the similarities in answers. The categories are put in short sentences to understand the response. The next phase is axial coding, where categories are presented in more detail to understand the first categories better. Axial coding is in the box after the verbal explanation.

Some questions do not include six responses from the CEOs. As the semi-structured method was used, there might be questions to which all the respondents did not respond. The flow of the interview took a different step, resulting in that all the question was not asked for everyone.

4.1 Information security

The interview started with questions relating to information security and more precisely cyber security, the training of the employees, and the responsibility for information security.

Question 1.
"What does information security mean to you?"

All six respondents had similar responses, and they categorized information security similarly in the responses. Responses and categories can be viewed below.

Responses to the question *"what does information security mean to you?"*	How the CEOs' responses can be categorised

"Two aspects exist, cyber security that we talk about and then there is information security. In my mind information security is a somewhat broader term, so, it also takes into account physical information such as those you store in papers and details you might throw in the rubbish, whereas cyber security is more occurring in cyberspace." *"Information security means the security which is handled by the human who is processing information and then security with technical measures. So, the human aspect and the technical aspect."* *"I see it as it is the human that is the weakest link when it comes to information security."*	Human aspect and technical
"Information security is like oil and if the oil is leaking, we can lose everything."	Potential existential threat to the company
"Information security is everything from physical security to cyber security. Securing your services and employees, and protecting the continuity of the company." *"Information security affects all operations on all levels."*	Something that is affecting the whole company

The categories listed above can be viewed as follows: CEOs think information security can be divided into two categories which are the human aspect and the technical aspect. The human aspect includes the ones who are using it, and the technological aspect includes e.g. devices. To concur with all the responses from the respondents, a CEO has to have knowledge of both aspects and realise that both of the categories are required to be aware by the employees of the company.

The second category that rose in all the responses was how participants considered that information security might affect the whole business when it is not well handled. Thus, information security is not merely one business unit inside the company, it is affecting the whole business, e.g. the employees, vendors, physical security, services, and the continuity of the company.

The third category which can be recognized from the responses is that CEOs are aware that when information security is not handled well, the worst-case scenario is the company may go into bankruptcy.

In axial coding the second and third categories are combined as they are both related to the same subject: information security affects the continuity of the business.

Axial coding from the categories:

Knowledge of information security	Affecting the continuity of the business

Question 2.
"*How important do you think information security is?"*

Four out of six participants responded to this question and their responses were all similar. The basic idea in all responses was that information security is a top priority and requires to be considered in everyday life. Below are the responses, and the categories collected from these responses.

Responses to the question: "*How important do you think information security is?"*	How the CEOs' responses can be categorised
"I think it is essential as the top priority. It should be on the agenda for the leadership as it is a truth that cyber threats are not decreasing, they are increasing. Therefore, it is of very high importance."	Top priority, high importance
"Basic essential and it needs to be in order. Whatever the size of the company it is known that it can destroy the company. It can be seen in everyday life in business if it is not thought to be important. Information security is affecting customer relations and all of our doings in general." *"Information security is important. Without information data security it would be impossible to operate."*	Need to be in order, important, and impossible to operate without it.

"Top priority. All the decisions, products, customer relations, need to be looked at from the point of view of information security."	Top priority, impossible to operate without information security.

This question was split into three categories viewed above. All the responses highlighted the importance of information security although they use different words to describe it. It becomes clear from the responses that CEOs recognize information security as something the company cannot operate without. One of the CEOs highlighted the importance of information security from the cyber security point of view by noting that cyber threats are not decreasing, they are increasing.

Axial coding from the categories:

Without information security, the company cannot operate

Question 3.

"Do you think companies recognise information security more as a cost of business than a necessity?

All the CEOs recognised information security as more as a cost of business than a necessity. Responses and the categories are presented below.

Responses to the question: *"Do you think companies recognise information security more as a cost of business than necessity?"*	How CEOs' responses can be categorised
"I would say that offices and facilities renting those are quite similar today. Information security is just something that needs to be conducted."	Cost of a business, hard to make a profit
"I guess a cost of business, of course, as there is the need to train the employees. At some level, this goes to the everyday life of the employee as well."	
"I think it is a cost for the business definitely, and it is hard to turn it around and make it profit-generating.	

Nevertheless, then if you consider it just a cost and you try to minimize it, you might be misreading the situation. You need to take it seriously and care about it. You need to handle it properly, therefore it requires investment and a serious approach."	Companies are not ready to make an effort for information security
"Unfortunately, companies do not think it is as important, they seem to think that someone will do it for them. Great examples like the Vastaamo-case exist and the challenges they have with it. Anyhow, companies are waking up to the need, even though, they are not ready to make an effort for it."	
"I think that when the GDPR came almost 3-4 years ago, that was when even the last CEOs thought that we should do something about information security."	
"Like a necessary cost, which is it though I have also compared it with physical security. You do not question the necessity to have locks on your doors, and maybe some key cards so you know who is who and who is not, or some other limitations such as who has access to some areas and who does not, e.g. at factories and research facilities."	Same cost as physical security

The responses above can imply that respondents think that the companies are not ready to put more effort into information security. One CEO is saying GDPR has brought more responsibilities for the companies, and when it came in the year 2016 numerous companies realised they are demanded to do more regarding information security.

According to one of the CEOs, Finland itself is a secure country which creates a false sense of security against international cybercrime. The CEO continues with a real-life example:

> *" IT-guy goes to the board and explains that we have these vulnerabilities, and we are exposed to some threats and ask for a budget to fix it. The board declines his proposal and says that we are focusing on these profit-generating initiatives first and after a month or so, the company got hacked and it was a ransomware attack."*

All the respondents brought up the case of Vastaamo at some point in the interview and pointed out that Vastaamo is an example that brought information security subject to be

more relevant to the companies. Still, as one of the CEOs is saying, some companies believe somebody else will do the information security for them.

Axial coding from the categories:

Information security is a necessary cost

Question 4.

"Do you think cyber security and data breaches are details to consider as a CEO?"

The response to this question from all the respondents was yes. Categories and reasons for the responses are listed below.

Responses to the question: *"Do you think cyber security and data breaches are details to consider as a CEO?"*	How CEOs' responses can be categorised
"Absolutely. When you learn some, you learn to be more scared, and even though I know in my heart that in our company employees are doing their best, and we establish the best possible security there. I know that is not going to hold if cyberattacks come from let's say foreign countries."	The absolute responsibility of the CEO, the employees' ability against foreign country attacks will not be enough
"Preparations are needed, just like insurance. Unfortunately in most cases, these details are considered after the attack has occurred. First to recover from the incident, and then make preparations for the next one. The company needs to have complete information security to cover the entire company." *"Yes, especially in information systems and infrastructure they need to be updated, so then you consider what has occurred before. Thus, on the surveillance side, that our company handles the security, in a small company, there might not be the capability. Thus, it is important to outsource to make sure everything is updated and there is a necessity for surveillance because these actions can occur fast."* *"Yes, those are considered and those occur almost daily. Somebody is trying to attack somebody, so it is an*	Learning from earlier mistakes, the company has to be prepared for an attack, details are considered only after the attack, systems demand to be updated, everyday defence, the need to outsource tasks

everyday defence and keep security up to date and information secure."	
"Cyber security attacks are a threat to each company. Every company is under a threat and every company has a presence in some way or another in a digital world. When you are in the digital world, nowadays everybody is, everybody is a threat to your company, and therefore you need to take it seriously. Also, there are legally bindings and regulated details that are forcing you to do that, in case you are not doing it, there might be some implications. "	Threat to each company, presence in a digital world, legally bindings

The CEOs all concurred that cyber threats and data breaches must be considered in today's business life. One of the CEOs presents that even though the employees are trained, a small company is not able to resist an attack coming from a foreign country. Another CEO said the threat is everywhere now as everyone is online with their devices all the time which makes companies and employees targets for attacks at all times and everywhere.

In the majority of the cases, the companies were not prepared for the attack. Consequently, security is considered after the attack and not before, as one of the CEOs is explaining. The systems must be updated and if the company has no resources for it themselves the company will outsource the service.

Axial coding from the categories:

Cyber security must be thought of before and not after an attack occurring

Question 5.

What do you think is more common, an insider threat or an outside threat to the company?

Responses to this question were in three different aspects. The majority of the respondents thought the threat was coming from inside the company. One respondent said the threat is more common from outside the company and one respondent said it is both.

The responses to the question: *What do you think is more common, an insider threat or an outside threat to the company?*	How CEOs' responses can be categorised
"Yes, I have seen this both in my career and personal life. Even though employees are the most asset value for the company, employees are also the weakest point. So, my response is the employees, and thus from inside the company." *"I believe the statistics are saying that most of the threats are coming from inside, due to human behaviour, however, sometimes consciously. I believe that kind of reception of the threat is coming from outside. However, I am not sure, as I do not have those statistics on top of my head at the moment."* *"If you think vulnerabilities or threats come from inside the company, fewer threats exist from the outside."* *"I would say inside since the data that is flowing has no value unless you know the context of the data. Data are only numbers, percentages, and details like that. So, you need to know the context to utilize it anyhow."*	Inside of the company
"Well, a threat usually comes from the outside, as it comes by using someone from the inside. Certainly, there are special cases where it is expedient. Usually, it is ignorance inside vulnerability, and exploitation from the outside. Mostly from the outside."	Outside of the company
"Probably depend on the company, as the larger the company, the greater the possibility that somebody from the inside might compromise you. However, if it is a small-, or medium-sized company then probably for those the threat is more from outside, and probably international. So, a two-sided response."	Both inside and outside of the company

The CEOs, who said that the threat has a greater possibility to come from inside the company, concurred that the inside threat is coming from the employees of the company. The threat might be conscious or unconsciously done. Usually, it is human behaviour that leads to vulnerabilities.

In the response to cyberattacks coming from outside the company, the CEO notifies that the threat is commonly coming from outside, as attackers are using someone from the inside to perform a cyberattack.

Based on the responses where the respondent chose both of the options, the response depends on the size of the company. One of the respondents' opinions is that in larger companies the threats are coming from inside, whereas in small,- and medium-sized companies threat is usually from the outside of the company.

Axial coding from the categories:

Inside threat	Outside threat	Both inside and outside

Question 6.

Do you think employees should be trained in information security?

One opinion was not possible to conclude from this question. All the CEOs concurred that training is important as it decreases human error and employees' awareness of the company's policies. All the responses are listed below with the categories of the responses.

The responses to the question: *Do you think employees should be trained in information security?*	How CEOs' responses can be categorised
"Training is extremely important as ignorance and lack of understanding create some human errors. With these human errors, threats are more likely to occur. There might be phishing in some e-mails or creating vulnerability to access control. As a part of general training, there is teaching how to use social media or IT equipment and at the same time noticing information threats".	Employees learn the new acts of phishing e-mails, important that the employees are aware of the company policy
"Training depends on the business field, this kind of general training. We are an industrial security service company, and we receive training straight from the public officer and it is useful training. The other part is the software developers. We decided that training for information security is best learned with the project conducted for customers."	

"Yes, of course. Training is useful and informs others about information security, especially the new ways of phishing information or trying to receive essential information or something. Some of them start to be quite useful. The demand for the training of the employees has increased so that they do not accidentally do anything stupid."	It decreases the human error, employees learn how to use social media or IT equipment
"Yes, definitely. I mean you train your employees for safety, and company policies, and then information security should be part of the company policy."	
"I have seen amazing pieces of training in terms of larger companies. They are using learning management tools and learning management systems. As a small,- and medium-sized company, I think that we do not have that much budget for building such a detail. Thus, now I think that the professionals, who are working especially in our business, have been trained in their schools, and they have courses."	

Training is important as it will affect the employees performing their tasks. When employees know the company's policies and when they are aware of the threats, a lower risk of being attacked occurs. When at the same time they are trained to use social media and IT equipment, the vulnerabilities of the company are less exposed.

Axial coding from the categories:

Training against cyber threats is highly important

Question number 7.
How would you train them?

The CEOs would train their employees with online courses, simulation tests, and sharing information among employees. The respondents' ideas of how they would train the employees are listed below with the categories. Three main categories were selected from the responses.

The responses to the question: *How would you train them?*	How CEOs' response can be categorised

"We have great development ops, operation team with 4-5 employees who are more professionals in this field, and they, usually send some e-mails or warnings, conveying in a Slack or Teams message that you should not fall into this trap here." *"Yes, pretty much online sharing information, about what is coming and going so that they are aware of this and that, meaning that internet platforms and Teams and others are used."*	Sharing information online
"Well, probably something that should be like a routine, like online courses work. However, there is some added value in doing actions physically, especially now that we are working in this hybrid model and some employees work outside the office. However, it could be a great idea to gather together in person and discuss it, and maybe do some exercises and view examples, even though it is a combination of many actions. Furthermore, I know that corporations use this phishing test, meaning that you let somebody send a phishing e-mail and check if an employee clicks it or not. Afterwards, those who clicked should be contacted and told that, by the way, this was a test and you failed. So, I think that those details add value." *"I think there are many publicly available educations available. Thus, the question is whether you as a company leader make it mandatory for your employees to be trained. With this publicly available education, I refer to many of these vendors who are providing digital systems like productivity tools, emails, calendar sheets, slides, and words. These vendors typically have a set of training that is related to security and how to handle those issues."*	Online course
"Training should be part of the work and as a part of daily/weekly information. In addition, there are different training programs, online or in real life. Then, of course, when we are in this business with information security services we do simulation tests, where we create a physical threat or information security threat." *"Then we have conducted simulation tests where we have ordered an attack to see the vulnerabilities."*	Simulation test

A few of the respondents would share information about information security online on different company channels. One of the companies had an operation team that would be in charge of sending the newest information about cyber security.

The majority of the respondents said they would organize online courses for their employees. One of the CEOs would like to receive information related to information security attacks in other companies, as it would be helpful for others to receive the information.

Two of the companies have had simulation tests where they ordered the attack for understanding where the vulnerabilities are for information security threats.

Axial coding from the categories:

Online course	Simulation tests	Operational team

Question 8.

If a cyberattack would occur in the company, who is responsible for it?

In the case of responsibility for a cyberattack in the company, the responses varied from the CEO to CTO. The responses and categories are listed below.

The responses to the question: *If a cyberattack would occur in the company, who is responsible for it*	How CEOs' responses can be categorised
"I think in the end, it is the CEO, that is why they are paid. They bear the responsibility, so they should organize information security in their company and ensure that employees are educated. However, in the end, everyone makes mistakes resulting in somebody then clicks the poor link or does something. In such a case, especially if it is intentional, then it is the perpetrator's fault, thus in the overall picture, I think in the end it is the CEO who is responsible. You might have a chief information security officer in your company if it is a larger, more organized company and then the CEO can delegate the tasks. However, you cannot delegate responsibility, that is the main idea. So, in the end, that is where the bus stops." *"In my opinion, every company should have a security manager, or at least when it comes to this cyberattack, let's say an information security manager. However, at the end of the day, every finger is pointing at the CEO, the owner of the company, or the acting CEO and even though there is an*	The CEO

information security manager, s/he is not fully responsible. Hence, everything that occurs is under the CEO's responsibility." *"At the end of the day, it is the CEO. Thus, the CEO is in charge of everything that occurs in the company, and he or she should be so well aware that those actions are more and more common. The CEO thinks of the company's resources to ensure that training is available and that there is security in place to minimize the threat. I do not mean that it is the CEO who knows about the training, however, it is the CEO who should point out resources for those types of actions."*	
"We have clear responsibilities. For information security, it is the executive leaders. Then we have an information security committee, and we have processes on how to handle incidents." *"The one responsible would be one of our technical leads. That kind of equal to CTO or somebody."* *"The responsible one is the executive team."*	Executive leaders, Chief Technical Officer (CTO)

Three out of six respondents said that the one, who is in charge or responsible if a company is a target of a cyberattack, would be the CEO. Two of the respondents told that the executive team, who the majority of the cases including a CEO, should be responsible. One of the respondents said that the technical team including the Chief technical officer should be accountable.

Consequently, all the CEOs think that the responsibility should be borne at an executive level, and the majority of them directly appointed a CEO to be responsible. They all stated that in the end, it is the CEO who is responsible. In general, it is the CEO who is in charge of information security in the majority of small companies.

Axial coding from the categories:

The CEO	Executive leaders	Chief of Technical Officer

4.2 Risk management

The second part of the interview concerned risk management focusing on information security. The questions are related to the meaning of the risk management, the risk management program, and the responsibility in risk management.

Question 1.
What does risk management mean to you?

Concerning responses to the question of the meaning of risk management, responses were similar to information security. The responses and the categories are listed below.

Responses to the question: *What does risk management mean to you?*	How CEOs' responses can be categorised
"Trying to keep up on the possible scenarios for what could go wrong, and what could occur and then you have scenarios on the table. Then, of course, make recovery plans and think about what should be conducted to avoid risk in advance. If a risk occurs, what should be conducted next. Of course, there are so many scenarios these days that it is difficult to make yourself ready for everything yet at least for most of the scenarios." *"Risk management starts from conceptualizing possible risks and then defining the level of the risks towards it. You have to make a plan on how to control the critical risks."*	Creating possible scenarios, making recovery plans for the company
"Risk management holistically means how we manage our company in the case of some very severe or less severe exception in the normal operation. Risks are something you should be prepared for as different scenarios could occur, and lots of those could be related to the digital environment, digital kind of data breach, or whatever ever occurs. Those risks should be considered well beforehand and somehow thought through that okay, how we can mitigate those though there are a lot of different risks."	How to manage a company in severe or less severe cases, digital environment plays a great part in today's business life.
"Risk management is preparing for the non-continuity of the business, such as a factory flaming into a fire and not functioning production. What is the level that which the company can take the risk? In the case of information security, it is usually ransomware. Are those the ones you can	Preparing for the continuity of the company.

fully prepare for the company risks beforehand? Over-reaction can also affect your business negatively."	
"We have recently taken risk management part in the daily life of our company. This year, as being the first year, we have been following risk management in our company. Of course, in the previous history, there were some documents where some employees have written something, though now we have a list and this is an active list that we are checking every month in our management meeting. Furthermore, we are reporting this risk management document to the members of the board, and they will check up if we have tackled all the risks and whether any risks have been raised, any risks going down or any risks settled. The list entails mainly business-related risks yet there are in the list also risks related to information security."	Risk management plan taken into account in a company, Reporting to the executive board is important
"From the start, in risk thinking, you have some probability and then you have some outcome. Risk thinking is a multiplier of probability and outcome so in risk management, first of all, you need to know or have some idea of what your risks are and what is the magnitude of them. Then you need to prioritize. As risk management can be, though, e.g. from an insurance perspective. As a private person, you have some risks that you recognize, e.g. you might own a car. If you count, there is a risk and that you should have insurance as a basic one. The starting point is that you evaluate what is the risk. What is your probability? What is the cost of the risk occurring? You cannot cover everything. You should pick the top ten and start from there. First of all, you should know your risk and then the second step is mitigating some risk. Risk mitigation strategy, what are the actual actions that you do?"	Probability and the outcome, priority of what risks to handle.

Risk management was considered setting the guides for businesses to stay stable and avoid threats from occurring. Companies are required to identify the vulnerabilities and know the threats which might occur towards those vulnerabilities. Risk management can be observed in the everyday life of the business and two companies had taken into account risk management guidelines as a main development subject for the company.

Axial coding from the categories:

To set the guides for business to stay stable	Avoid threats from occurring

Question 2.

Do you think that risk management is an important part of the company?

The second question for risk management is the importance of risk management for the company. The majority of the responses were similar to the responses to information security. Responses can be seen below.

The responses to the question: *do you think that risk management is an important part of the company?*	How CEOs' responses can be categorised
"We have really strict project management where employees are following their work, and we are using strong models. Retrospect team meetings are arranged occasionally. So, I think the information in that field is moving fast, and then, to be honest, I somehow think risk management lists are a pain for the CEO at least. However, it is another list we need to follow. I feel it would be more beneficial to sit down and then and just look directly at the cyberattacks occurring or information security breaches and maybe learn what has occurred in another company. I have heard some stories, not like us filling the list all the time, that it can lead to the position that we are focusing only on our company and our list and feel secure, though what is the reality."	A Risk management list is just another list for the CEO to fill in, not as beneficial as discussing with employees.
"Business is all about taking a risk and taking a positive risk. So, if you shield yourself from all the risks and hide in the corner nothing occurs. However, the risk is two-sided, you might have some negative risks. Thus, more often a negative than positive risk and there are details you cannot do to affect the positive outcome. Then you should have some kind of risk management. Starting from one-man shows like me, I have some risk management as I have insurance. I consider everything yet not everything is documented. Only me I am documenting the actions. Thus, even if it is a one-person organization, it might be a great idea to document something, as that is how you process it. Some risk management should be in place and then when it comes to information security, it should not be separate from risk management. Information security is just one aspect and one new kind of threat that your company faces. Yeah, it should be somehow thought of."	Business is all about taking a risk, Documentation should be conducted, information security is a part of risk management
"This is quite the same as the previous question. Without risk management, the company cannot be led. For this case, we have insurance to make sure about the continuity of the company."	Insurances

"Definitely, in the last board meeting, we took it to the table and decided that at the beginning of next year we will have a risk management program, risk reviewing workshop, and we try to capture what are the risks and how we can mitigate them and how should we use resources if we see that some are more probable to occur than others."	The company will create a risk management review workshop
"For us, demands for risk management come through a governmental project and risk management needs to be thought of through the annual reporting to the board of directors. The case Vastaamo raises demands from our customers and documentation."	Governmental and executive board demands risk management.
"Risk management is important yet maybe not be something that is a daily object. Based on more or less on technical systems. In some way more to our operating models, when a new service is set up or something like that. However, it is quite important for the process."	Is important yet not a daily object, more to the technical systems.

Risk management demands are considered necessary for the company to be successful. Thus, the company has to be prepared for the threats. One of the CEOs is describing how the risk management list might not be the best solution for companies as it is collecting the risks for a specific company. The CEO continues that it would be more beneficial to know the threats occurring in another company.

Axial coding from the categories:

Risk management demands are necessary for the company to be successful

Question number 3.

Are employees aware of the risk management program?

All the CEOs' responded that employees are aware of the company's risk management program. The responses to this question can be viewed as CEOs' ideas of how well the employees are aware of risk management programs.

The responses to the question: *Are employees aware of the risk management program?*	How CEOs' responses can be categorised

"Employees are a part of the process of business continuity, so yes."	Yes, employees are part of the continuity plan
"Definitely, in the last board meeting, we took it to the table and decided that at the beginning of next year we will have risk management, risk reviewing workshop, and we try to capture what are the risks and how can we mitigate them in the best possible way and how should we use resources if we see that some risks are more probable to occur than the others."	Yes, a risk management review workshop is created
"Yes, I started two months ago and I can see many actions are not well considered. I believe employees are to a certain extent aware that there are situations that could be improved."	Yes, still there is room for improvement
"or us, the demands come with Katakri, and we need to examine this in our yearly report with the board. We think of different risks and not only with the information security, however, also risks with employees and services. Of course, the case of Vastaamo brought more demands from our customers' side, and we need to be on the front line with the right documentation that demands that our risks are identified. So, it affects every level."	Yes, the level of awareness in risk management includes employees
"Hopefully yes, should be. We discuss whether we are going to the fairs in New York and whether we are going to the same plane or with a different, all the eggs are not in one basket."	Yes, there is a discussion with the employees
"Yeah, at least with the policies they are certain of and with the quality system."	Yes, employees are aware of the policies

In the responses to the question of employees' awareness of the company's risk management program, all the CEOs responded yes. Two of the companies had taken risk management programs to be one of the top priorities for the ongoing year. Based on the responses the CEOs seem confident that their employees are aware of the company's risk management as the risk management determines the company's continuity and most of the actions on risk management are part of the employees' everyday tasks.

Axial coding from the categories:

Yes, employees are aware of the company's risk management

Question number 4.

Do you think it is the CEO who does the guidelines for risk management?

All the companies had thought of risk management programs. Risk management is executed on different levels and entails different demands in all the companies. From the responses, it can be implied that there is no clear understanding as to who is making the guidelines for the company. Responses and their categorization can be seen below.

The responses to the question: *Do you think it is the CEO who does the guidelines for risk management?*	How CEOs' responses can be categorised
"I would say in the end, it is the CEO who is responsible also for taking cyber security into account. However, the way the CEO might handle details does not necessarily mean that the CEO him/herself fixes everything. A CEO just needs to facilitate the organization so that these details occur. A CEO bears a large chunk of the responsibility and if something goes wrong, s/he should take responsibility, and it is quite a poor policy to blame others as you are the head of the company. So, in that sense, the CEO yes, although like I said, a CEO should consider how to build the culture around the company. So, you lead on different levels, meaning that s/he provides a culture that takes risk into account or health into account or whichever part of the business domains you might need. Moreover, if you recognize that you need somebody to work on an issue, then a CEO hires somebody or organizes it otherwise. In that sense, you are responsible, yet you are not necessarily a day-to-day hands-on approach to those details."	The CEO
"No, we have been doing this as a team. The team was established by the management team. So, there is the HR director and the quality engineer, finance production managers, and me. To be honest, this information security and cyberattack in this field is a great cash flow for businesses. Even though information security is a great idea yet it is that they are marketing this with fear and I kind of hate that."	A team

"There has been some already in place before I stepped in. Then, of course, some of those we already adjusted. A matrix exists of whom can do and what, and who is in charge of and what type of details."	Matrix of whom can do what
"I approve, revise and it is up to those who have more substantial knowledge and competence to offer guidance."	The CEO
"It depends on the size of the company. The CEO is responsible, and s/he will obligate someone to be responsible for the quality,- or risk management, or work for the safety committee."	The CEO
"Well, I am the responsible one as a CEO. Then who performs the actual action depends on whether it is software development or equipment, or from our IT department. In those departments, there are other employees involved."	The CEO

For the majority of the companies, a CEO makes the last marks for the program and checks all the necessary information is in place. According to one of the CEOs, he will revise the guidelines and someone else from the company had issued them. For one company, risk management guidelines were executed as teamwork with representatives from different departments of the organization. One of the companies used a matrix presenting responsibilities and the risk management program was created using the matrix.

Axial coding from the categories:

The CEO	A matrix	A team

Question 5.

What are the greatest assets for the company?

Acknowledging the assets of the company and the company's vulnerabilities are important. The responses of what are the greatest assets for the company are listed and categorized below.

The responses to the question: *What are the greatest assets for the company?*	How CEOs' responses can be categorised

"If I had to pick one, I would say it is the employees that you manage to gather for the company. If you have a poor team, everything fails."	Employees
"The employees, of course. The big data, we are delivering all the data of what customers are using. Even though the customers own the product, details like that are gold."	Employees, big data
"The greatest asset has to be the key people. I will not say that all the personnel is an asset. There are a lot of useful employees, some are average and a few poor ones are there usually as well. Another asset is the product and service that the customers are ready to pay for."	Key persons, product & service
"Our assets are the employees who are working for us. That is the widest I would say. The knowledge they have and what their experience is, and what they know about the industry. Then our other asset is our customers, of course. They are continually using our services every month. Thus, of course, our employees, our customers are our assets, and then we have some intellectual property assets as well."	Employees, customers, intellectuality
"Our reputation is one of our greatest assets. Reputation and credibility. Also, recognizability and of course personnel is the one that is creating a reputation. Conclusively, personnel, reputation, and credibility are the greatest assets."	Reputation, credibility, and reorganization
"Employees"	Employees

All the respondents stated that employees are their greatest assets. Additionally, customers, credibility, reputation, reorganization, intellectuality, product, service, and big data were mentioned.

Axial coding from the categories:

Employees

Question 6.

If an action is executed by an employee who results in an incomplete or non-existent policy and will affect negative the company, who is the person to blame for it?

The responses to the question of the responsibility of an action executed after a non-existent policy will put a company in the negative spotlight, all the responses were the CEO. The explanations behind the responses are listed below.

The responses to the question*: If an action is executed by an employee who results in an incomplete or non-existent policy and will affect negative the company, who is the person to blame for it?*	How CEOs' responses can be categorised
"Different layers exist. I am not the best one to keep reminding myself of my own mistakes, as I believe I have been falling into one cyberattack as well in my career. I receive all the viruses into our network, and my laptop went crazy and I lost it totally as the hardware was full of viruses. That was an unpleasant moment yet it seems that we were ready for those issues to occur. So, those occurred three to four times in my time as the CEO, and the attackers are evolving to be better and better with these phishing attempts and these "please click this link here"- emails. I think that all the professionals are falling into this and not the regular office workers. The professionals are "I know this, I can do it." I was talking about the layers. So, this was the easiest one. The hardest ones are those leaks and breaches where it touches customers. We have the responsibility to make an announcement, and we have conducted it twice. I believe that is a storm for the company. Although we need to conduct the announcement and it is our responsibility, and we have conducted it. I think the process that we have planned has worked fine and nicely."	The CEO
"Well, it is the CEO who is in charge of everything and this case. In these public information security issues, it is the CEO who is in charge, even though there would be someone else obligated to do it. From this question comes also the question of the crisis communication and how it is handled and if the company is ready for the worst-case scenario."	The CEO
"Yes, who would be the blame, I think the blame would go to the person him/herself. Then who would handle the consequences would be the management of the company, whoever it is. Some people are near the company, those that it hits and then there is ultimately the CEO who it hits as well. In most cases, it requires some kind of attention and comments and some kind of nurturing."	The CEO

"In the end, it is the CEO."	The CEO
"*Then it is, of course, the management team and in the end myself."*	The CEO

All the participants responded that in the end, the one responsible for the action executed after a non-existent policy is the CEO.

Axial coding from the categories:

The CEO

4.3 The role of the CEO

In this chapter are two questions presented that are related to the CEO's role in the company. Questions and respondents' responses are categorised to see the similarities and differences in the responses.

Question 1.
Do you think CEO can be the imperial CEO which means that at the same time be the CEO of the company and the chairman of the board of directors?

The responses to the question are divided into three categories. One of the CEOs thought that an imperial CEO is a useful idea, three CEOs thought it was a negative idea, and two of the CEOs had neutral thoughts on the subject. CEOs' responses and categories are listed below.

The responses to the question: *Do you think CEO can be the imperial CEO which means that at the same time be the CEO of the company and the chairman of the board of directors?*	How CEOs' responses can be categorised
"Well, I am the solo owner, the chairman, the CEO, and the only person working. I take my influence from other peers. I think it is fantastic. I do not need to submit anything to anybody. Everything is my decision and that is actually why I would be reluctant to sell some part of my company to receive	Great idea to be imperial CEO

some money. I would consider it much before I would take some investors. It should be a very prime reason for that. A risk exists that you are too full of yourself, and start soloing, and probably that sometimes occurs. However, that occurs in larger organizations as well. I know some leaders forget to listen to others and forget they are not the smartest person on earth, or smarter than all the rest of the humans combined. So, when you keep that in mind, I think it is a great idea. It makes it more dynamic and decision-making is straightforward when you are aware of something you want to pursue and you recognize your demand to change the course, you can do it. You do not have to convince others. In that sense, it is great, and then for me, it is ideal that you know some advisors, who are not too involved, yet they speak their minds. For me it works, for others, it might not. It is a different story when you are doing business with somebody else's money. Then you are not an entrepreneur in that sense anymore as you are working for others, and that is something that is on my value ladder quite high. That is the reason why I started my business, to be more self-reliant. Thus, I do not know, maybe that will change at some point."	
"We had a previous history with the imperial CEO. 20 years ago, there was this kind of situation. The moment when the person jumped to be a board member and head of the board, changes occurred. I want to raise a third detail. Stakeholding and being an owner. I think the member of the board needs to be minor owners, and the main owners need to be somewhere else. The management team and team of directors in the business and a CEO need to own something in the mid-sized company as then the passion will be there. Also, the responsibilities, it is the best when your home loans and security are detached from the company. However, a CEO and head of the board, and the owner cannot be the same person. Then the questions inside of your head would be "as an owner what do I think, as a member of the board what do I think? As an acting CEO and taking care of all the operational employees what I think?" three different people are thinking inside of your head." *"I would say it is incompetence. The reason why I am saying this is that there cannot be just one person who executes everything. I do understand that in micro-companies, so to speak less than ten employees working, the situation might be like this. It would be wise to build a larger organization so that the CEO would not be a member of the board of directors, as s/he could be in the board meetings as a CEO giving the information to the board. In our company, the main owner is the head of the board of directors, s/he is not involved in the daily operations. I could see that members of the board of*	An imperial CEO is not a great idea

directors are outside of the company. I am the minor owner and I am a member of the board. I consider my role as a member of a board even though I am an owner. However, I have the hat of the owner, the hat of the member of the board, and the hat of the CEO. You have to be able to separate these hats." *"I think it is somewhat negative. We used to have that when starting our company. However, it is better to have as professionals as possible and term the roles apart, it should not be the CEO. It takes the company faster and further if the board and the CEO are different roles."*	
" Well, in Nordic countries it is noticed negatively as in that situation the CEO is reporting to him/herself. The role of the CEO depends on the head of the board of directors and the owner of the company. In larger companies, such as the size of Nokia or the American stock company, it is a typical idea of the imperial CEO and now it is seen also at some level in Finnish smaller companies, usually resulting in the ownership. The CEO is the founder and largest owner and the head of the board of directors, however then if there are private equity investors, the board demands to separate the roles." *" I am pretty neutral to that. I mean if you are an entrepreneur and you founded the company and you are in that chairman position yet then you are in a CEO position as well and you are willing to listen to more experienced ones in certain areas, then it is a totally fine detail. However, in case you have twisted your mind as being the chairman and the CEO, then it is complicated. I have seen that type of CEO as well."*	Neutral ideas of using an imperial CEO

The CEOs that thought of an imperial CEO as a negative idea were concurring that when a CEO has many hats to wear, A CEO hat and the hat of the head of the board of directors, decision-making becomes more difficult as at some point the CEO is responsible for her/himself. A chance is also that an imperial CEO will become too powerful and use the status hastily.

The CEO who had positive thoughts had experienced being the imperial CEO. In a smaller business, it functions as there is only one person who the CEO is accountable for, him/herself. The CEO realizes there might be some drawbacks to the decisions that reflect the success of the company.

The two CEOs who had neutral thoughts were certain that the imperial CEO functions in the smaller companies when there are not as many employees as in larger companies.

Axial coding from the categories:

Not a great idea	Great idea	Neural thoughts

Question 2.

What are the best qualities for the CEO?

The responses to this question were quite wide, though there are similarities revealed in the responses. The qualities that almost every CEO responds to are delegating, listening, seeing to the future, and the demand for growing the business. Responses and categories are listed below.

Responses to the question: *What are the best qualities for the CEO?*	How CEOs' responses can be categorised
" This is my first CEO job and before I join, for three years now, I thought that there was a personality type or there are only a few that will manage as a CEO. However, now I have seen so much and I have experienced so many kinds of ways of executing details. I have seen CEOs who are extroverts, I have seen CEOs who have been introverts. I think that there is no prescription for what kind of person can be a great CEO. However, I think it is more about the knowledge and the passion, and the information about the field you are working in. There are great studies of the listed CEOs in large-cap, mid-cap, and first north lists, and the varieties of the personalities are huge. Thus, I would love to see more of another gender than males in this position. I know a lot of female CEOs and I think that in the management work they are somehow better in those fields. They are also better at innovation which has been proved in many cases and studies. At least the CEO needs to be a person who believes himself/herself and knows what to do and a person who can make a life of a strategy and the plans and what the board members have been dreaming of, and the stakeholders as well. I think that it can variate greatly who can be a great CEO of the company."	More about the knowledge and the passion, believe him/herself, can make strategies and plans

"A CEO needs to have the executive capacity and be able to create strategy with the board. A CEO needs to have a vision of where the company is headed. However, the vision is needed to bring into everyday life in the work environment and have the measures to see how the company is doing. There are two kinds of CEOs, visionaries and integrators. They are both needed."	Executive capacity, being able to create a strategy, visions
"Well, it is tough as you need to have some mixed qualities. You need to be self-assured and have faith in what you are doing, and then even quite bold. However, you need to be a great listener and you need to be roughly open to others' opinions and be critical about your doings at the same time. You need to be leaning forward yet also retain some sense of yourself. Thus, learn to be somehow cautious. It depends on the stage of the company, and what kind of CEO you need. However, I would say that the CEO needs somehow to be able to think forward. You are lost to day in and day out findings, and the mandatory issues and there is a risk that you just lose yourself there. So you need to be able to recognize that stuff and think ahead. You need to be able to create some vision and if not, you need to be able to find someone who helps you receive that vision. You need to be able to conduct actions through others or somehow be able to outsource the ideas from your head to actualize by others. The employees working in your company or companies on your network or however you organize it, you need to be able to organize it. Then somehow delegate issues, as otherwise there is going to be just one and you not going to scale, if that is your goal, then fine. Thus, if we are talking about some company that has aimed to grow or even has grown to some extent you need to run it. You have to be able to multiply yourself, somehow and the best way is to push and delegate them to others and trust that details are conducted if not, then you step in. Although if trust is not existing and you just delegate and you run after those details, again you are busy. You need to be brave, humble, and then a great organizer."	Be self-reassurance, have faith, bold, great listener, open to others' opinions and critical thinking, think forward, be able to delegate,
"Great listening skills and empathy are important. Then after this, some kind of generalist. A very high level of technicality is not a great detail, or not being very great at sales or not very great at financial accounting. CEO needs to be a kind of generalist that is not very great at anything though can understand the principles of various sectors. A CEO has the motivation to learn those stuff, if not already have learned. I would say that it is important that as easily you are too technical, you do not understand finances, you are not achieving development. However, managing is the kind of	Great listener, empathy, generalist, motivation to learn new, can make compromises

listening and trying to understand a bit of everything and making compromises."	
"The best qualities for a CEO depend on the field of the business and its size. A CEO needs to be able to make decisions and commit to those ideas. To be able to grow the business, not only with its capabilities, however, also with information security issues, and risk management. A CEO needs to be bullheaded and be able to offer negative feedback. However, the CEO has to be able to act as CEO even though the economic situation is not that well."	Able to make decisions, commit to ideas, able to grow the business, bullheaded, and able to offer negative feedback

One of the best qualities that the CEOs listed were that a CEO can make decisions, be able to grow the business, be able to offer feedback, great listener, be open to others' opinions, and see into the future. All these qualities are needed to be able to manage a business and to be able to grow a business. Everyone is not able to be a CEO, no certain type exists as there are several qualities needed for the CEO to be successful. Some qualities come by nature, yet some of them can be learned.

Axial coding from the categories:

Delegating	Listening to others	Being able to see into the future

5 DISCUSSION

Results of the entire interview are presented, analysed, and viewed in Chapter 5. The three parts of the interview are summarised together as one to have a better understanding about the entire interview with the selected CEOs. In this discussion is also the last category of the grounded theory presented which is selective coding. Selective coding creates the theory for this master's thesis and concludes all the responses to one theory. Selective coding is demonstrates at the end of all the chapters as a textbox.

All the questions are not presented here, however, they will support the discussion chapter and presents a broader perspective to the role of the CEO in a company's information security.

5.1 The importance of IS & risk management

The interview started with a question about the basic idea of information security. All the respondents thought that the meaning of information security is broad. The CEOs identified information security in two different aspects, referring to both the technology we use and the users of the technology, e.g. the employees of the company. The technology aspect can be divided into physical security, the one hand referring to locks, doors, and walls, and other hand referring to cyber security which is the security of online interactions. Information security is a broader aspect at a company level that covers the governance of information. Thus, the definition of information security by Iannarelli & O'Shaughnessy (2014), is a more extensive entity than an IT problem, it consists of systemic solutions to counteract threats, alleviate inefficiencies, and prepare for the future. Preparing for the future is what respondents found important as they all concurred that lack of information security can destroy the whole company and affect the company's continuity. As can be viewed from the definition of Iannarelli & O'Shaughnessy and the participants' responses, both theory, and practice imply that information security affects the whole business and the manner the company is handled. One of the CEOs described how the importance of information security is thought throughout all the activities in the company. Taking into consideration the company's culture, especially the culture of security inside the company, the CEO has to require all

the employees' awareness of risk management. In the responses, all the CEOs confirm that they are certain of their employees are aware of the risk management and that the company has information flowing about the cyberattacks that could occur.
For the question about the importance of information security, all the respondents responded that it is highly important for a company. Without information security, it would be impossible to function as a company. Another question was about the meaning of corporate risk management and the responses were quite similar to information security related question. Without corporate risk management, the continuity of the company is at risk. Risk management includes creating possible scenarios and recovery plans for the company. Risk management includes information security and identifying vulnerabilities and the threats against those vulnerabilities. There are many risk management processes to use how to identify vulnerabilities and one of them is by Bojanc & Jermain- Blažič (2013).

Selective coding:

Risk management including information security, aims the company to prepare for the future and the threats it might have and it also highly affects the continuity of the business. Employees' awareness of risk management programs is a key element that will affect the future of the business.

5.1.1 The occurrence of information security

One of the respondents' told his opinions on why companies do not think that information security is as important as it should. The CEO thinks that companies have not yet realized the scale of international cybercrime, and how organized it is. The CEO continues that the phenomena of phishing attacks and phony phone calls have increased during the Corona pandemic. According to one of the CEOs, companies in Finland started to wake up as greater incidents in Finland are occurring. In Finland companies still seems to believe that while cyberattacks are increasingly occurring, such will not occur to us. According to one of the CEOs, as Finland itself is a secure country, it creates a false sense of security against international cybercrime. All the respondents mention the Vastaamo case (Yle, 2020) which influenced the information security in Finnish companies, and brought awareness of the cyberattacks on the companies to the public.

Huaman et al. (2021) researched medium-sized companies in Germany and concurred that the companies have their basic knowledge about the company including its risk and threats. At a company level, they have awareness of the security, but information has not reached all the employees of the company. The responses of the CEOs imply that the same applies to small IT companies in Finland. They know that cyber security threats are occurring, but they are not fully prepared for them.
According to one of the respondents, the effect of GDPR coming in 2016 can be observed in the business field. GDPR was the last wake-up call for CEOs to realize that there is information security related tasks that need to be executed in every business sector.

One of the CEOs thinks that it is a shame that information security is advertised with fear. For the future, the CEO hopes there would be an open environment, e.g. a platform where companies could share the attacks that have occurred in their company and this would share the awareness and knowledge to other companies. The culture today is more that the companies do not share the incidents if it is not regulated by the government to do so.

Selective coding:

Finnish small-sized companies have not yet realize that the threat is real and is possible to occur any of the companies.

5.1.2 How the size of the company affects

The report executed by the UK Department of Digital, Culture, Media & Sports (2019) has concluded that 32 % of the businesses had experienced cyber security breaches or attacks in the past 12 months. For the majority of the respondents of this research interview, at least phishing attempts were an everyday subject. One of the respondents highlighted that the importance of information security comes from the fact that cyber security threats are not decreasing, they are increasing. As can be viewed from the responses, it is not only medium-sized companies that are one of the best options for cyberattacks. All sizes of companies are in danger of being targeted for an attack every day. According to Iannarelly & O'shaughnessy (2014), medium-sized companies are the best for cyberattacks size-wise. All the participating companies were small-sized companies and all the CEOs told that they need to consider cyber threats every day.

From this, can conclude that today, all the companies might be targeted for cyberattacks and not only medium-sized companies.

Selective coding:

Cyber threats are increasing and they affect companies of all sizes

5.2 Inside threat vs outside threat

Four out of six CEOs responded that it is usually an inside threat that occurs. The CEOs realize that the reason for the inside threat is usually human behaviour, i.e. human error and it is one of the employees who have made a mistake. According to Colwill (2010) far less factual data exist on inside attacks and the majority of the incidents occurring inside the company are accidents. The companies are also aware of inside threats that might occur, yet they are not aware of how to act against those. More information exists on outside threats.

One of the CEO said that it is usually an outside threat though they are using an insider to create a threat, e.g. a phishing attempt where someone has clicked a link that was not to be clicked. This is resulting in the fact that attackers are evolving to be clever and it is not as easy for users to recognize which attacks are real and which are not.
One of the respondents said that usually, the size of the company matters where the attack is coming from. For larger companies, there is a larger possibility that it comes from the inside as an employee executing some act. As a small,- and medium-sized company it is usually the attack from the outside.

Selective coding:

The threat is usually an inside threat when a human error occurs

5.3 The cost of information security

To the question whether information security is considered more as a cost of business than a necessity, all the respondents concurred that it is a cost of business. Furthermore,

one of the CEOs thinks that cyber security is a cost that is hard to turn into a profit. According to the CEO, when the company is trying to minimize the cost, it is misleading the situation. Using investment for information security is an issue that has to be taken seriously. According to Coburn (2018), information security has to be seen as preventing cyberattacks and preventing risk for different losses a company might encounter with.

Another respondent stated that, the main cost comes from educating the employees. Educating the employees minimizes the risk of human error occurring. As one of the CEO was telling, educating employees will help them identify the acts of phishing attempts. Additionally, a CEO pointed out that information security is part of employees' everyday life, as information security is important and affects personal life simultaneously with business life. There were almost the same responses to the question of employees' awareness of risk management. Raising awareness creates more knowledge for the employees, yet as one of the CEOs replied there is typically room for improvement and there is not enough awareness when it comes to information security or risk management. Most of the CEOs had the mindset that the employees already know much about risk management in the company as it is so tightly part of private life, and risk management is nowadays already learned in school.

One of the CEOs responded that information security requires to be executed and a majority of the companies think someone will execute information security for them. The companies not realizing the actions required to be taken before an attack or breach occurs. This results in that companies will not make as much effort into information security as the effort they put on physical security e.g. locks and accessibility.

According to one of the respondents, the effect of GDPR in the year 2016 can be observed in the business field. GDPR was the last wake-up call for CEOs to realize that there are issues that need to be executed in every business sector.

Selective coding:

Companies think that information security is more of a cost for the business than a necessity. Companies do not put enough effort into information security and then it is usually too late and the attack has already occurred. For information security, educating employees is highly important.

5.4 Risk management VS information security

When it came to risk management, none of the respondents questioned whether having locks in the facility doors and that these security matters are of utmost importance. Consequently, physical security is not doubted as much as cyber security. It seems that when the security measures in information security are not seen with their own eyes and are not understood in the same security measures, protection is not as simple.

The question of whom would be responsible if there would be a cyberattack in the company divided the responses into different responses. Three out of six CEOs responded that in that case, it would be the CEO who is responsible. Two of the CEOs responded that it would be an executive team, which includes the CEO yet it is not only the CEO. One of the CEOs responded that it would be a Chief of Technical officer (CTO) who would be responsible. As can be seen, there is no clear knowledge of a case of a cyberattack and who is accountable.

The question of risk management when some employee executes an action that would put the company in a negative light, all the CEOs responded that the one responsible for the action would be the CEO. In a conclusion, it can be seen as when there is an IT-related risk such as a cyber security threat it is not necessarily a CEO who is responsible although when the act is more communal the responsible one is a CEO. According to Speed (2011), a C-level manager is accountable for the damages if it is a result of an incomplete or non-existing policy. From the responses can be noticed that all the CEOs concurred with responses when it came to risk management responsibility. When discussing cyberattacks responsibility, there was variation in the responses.

Based on the results of the CEOs it appears that when comparing risk management and information security, there is not as much awareness about information security as there is in risk management. The variation in response to the occurrence of cyberattacks and the accountability of those attacks indicates that awareness of information security is not at the same level as with risk management. Several CEOs during the interview commented that they are not the experts when it comes to information security and cyberattacks.

Selective coding:

When comparing information security and risk management the awareness of risk management is higher than information security. When asked about the responsibility in risk management, the response was the CEO, however, in information security, there was variation in response.

5.5.1 Company's greatest assets

In the response to the question about what are the greatest assets for the company, all the CEOs responded it is the employees of the company. CEOs are aware that it is the employees who make the company successful and without them, the company would not function in the way it is functioning now. When talking about cyber security and risk management, CEOs responded that they are aware that human behaviour, especially employees action is the weakest point that can cause a cyberattack in the company. Some CEOs understood that there is not enough awareness among employees when it comes to cyberattacks, yet CEOs were certain that employees are aware of the company's risk management. According to Colwill (2010), the risk of human behaviour must be explicitly taken into account in risk management. In conclusion, these CEOs respond that their company's greatest asset is employees, however, at the same time, human behaviour is a great risk in cyber security threats.

Other assets that the CEOs listed were big data, products & services, customers, intellectuality, reputation, credibility, and reorganization. All the assets mentioned above will guarantee the company's success, and they are all thanks to teamwork and that is something that can be educated to the employees. Some of them such as credibility are something that comes from the employees by nature.

Selective coding:

Employees are the greatest asset for the companies, yet they are the weakest link and create the human error for cyberattacks.

5.6 The CEO's responsibility in the company

The third part of the interview was about the CEO's role in the company. Responses to the question of imperial CEO variate from each other. Three out of the six CEOs responded that it is not a great idea to have an imperial CEO. Most of the CEOs had experience working with imperial CEO. Their reason for imperial CEO not being a great idea was that there certainly cannot be one person who can execute everything. When the imperial CEO is acting as CEO and the head of the board of directors there are multiple hats s/he is wearing. Wearing multiple hats is what is creating a problem with decision-making. The CEOs continue that usually, it is better management when the head of the board of directors is not involved in the everyday life of the company. According to Green (2004), not all CEOs take advantage of the position, and usually, a CEO wants to make a decision that benefits the company.

One of the CEOs stated that his thoughts about imperial CEOs were quite neutral. In his mind, it is common in Nordic countries to notice an imperial CEO as a negative as then the CEO is reporting to him/herself. The CEO continues that usually in the larger companies, especially in US imperial CEOs are common. Nowadays imperial CEOs are becoming more common in Finnish small-sized companies. In smaller companies, there are not as many members on the board of directors which results in the CEO being the head of the board of directors. Another CEO has neutral thoughts also about an imperial CEO. The CEO has seen what can occur if the imperial CEO have been twisted with his/hers mind. If that occurs, the management of the company becomes complicated.

One of the CEOs had a positive thought of an imperial CEO. The CEO has experience of being an imperial CEO as his company is solo-owned with a partner company. The CEO sees it as freedom, as there is no need to submit to anybody. The CEO realizes the risk that an imperial CEO might become too powerful to the point that it is affecting negative affects the company. The CEO is comparing larger companies where the same occurs.

Selective coding:

An imperial CEO is mostly seen negative light as the CEO has too much power to him/herself. An imperial CEO is common in a smaller companies with less employees.

5.6.1 Best qualities for the CEO

Responses to the question of what are the best qualities for a CEO the topics of the responses were quite the same as with some variation. By Gainess-Ross (2000), the best qualities for a CEO are CEO's awareness of the company's visions and values, realizing the company is discoverable, must bring the vision and strategy in an understandable aspect, understand wort-of-mouth and online talk, lead strong management team, decision making and risk taking and the demand of the stakeholders. A CEO is demanded passion for the work and s/he has to believe him/herself. A CEO has to be a strategic person, one who can create strategies and see them already in the future. Listening to the employees is one of the most important qualities for a CEO. With listening, a CEO has to be open to others' opinions and ideas. Delegating and making compromises are one of the qualities mentioned. Without those qualities, it is more difficult to manage the company as a CEO is not able to execute everything. A CEO has to have a vision for the future and see into the future and not live in the current day. A CEO has to keep in mind the growth of the company. Giving and receiving feedback, positive and negative is most important for a CEO.

Selective coding:

The best qualities for a CEO are passion for work, to be able to see in the future, delegating and listening to other.

6 CONCLUSION

Chapter 6. presents the conclusion for this master's thesis. A short restatement of the research questions and presentation of the key arguments. A short discussion about the implications of this research is stated. The conclusion finishes with the limitation and future suggestions for this master's research.

The core aim of this study was to understand the responsibilities of the CEO toward information security and corporate risk management. This topic was researched from the perspective of the CEO. With the research questions were desired to understand how the CEOs realise the information security and the corporate risk management and the responsibilities they create for the company.

6.1 Research questions and discussion

Cyberattacks and data breaches are targeting companies now and in the future. The interest of this master's research was to gain knowledge from the CEO's perspective on the management of information security and risk management. The main research questions were:

- *Who would be responsible if there would occur a cyberattack in the company?*
- *If an action is executed by an employee as an incomplete or non-existent policy and that action affects negative the company, who is responsible for it?*

The first one is related to information security and the second to risk management.

As the results implicate, when discussing the responsibility with information security, there was a difference in responses that concludes that there is not as much awareness of the responsibilities as there is in the responses to risk management. To the second question, responsibilities in risk management, all the respondents answer the CEO.
At the same time, the CEOs were certain that employees are aware of the company's risk management program, they also realize that employees are their weakest link against cyberattacks which usually are foreign attacks.

All the CEOs also concurred that the need for information security is arising as the number of cyberattacks and data breaches are increasing. All the CEOs were certain that

the employees of the company are aware of the company's risk management guidelines, yet when it came to cyberattacks, the information and knowledge the employees' have, is not enough, especially against a foreign attack.

The difference between information security and risk management entails that when it came to physical security, e.g. having locks on your door, no one is questioning that. However, when it is about information security the necessity is not as coherent. The last observation of the results is that in the Finnish companies' information security is seen more as a cost of business than a necessity. Companies usually think more of information security after an attack has occurred, not before as it should be. As the companies do not think that the attack could occur to them, they are not prepared for an attack to occur which leads companies to be easy targets for attackers.

6.2 Limitations and future studies

The conducted study has limitations. The first limitation is the small number of participants. With a larger sample size, the results would be more reliable and would demonstrate more representative results.

One of the limitations was also that the researcher wanted to have participants from medium-sized companies, as it is stated as one of the characteristics of the sampling method. Unfortunately, there were none of the CEOs responded to the message asking to participate in the interview. This limits the scope to the small-size companies and no small,- and medium-sized companies.

Another limitation is the part of the interview about the role of the CEO. It has been included in the master's thesis to gain more knowledge of the CEOs' ideas as they are respondents in the interview. However, the subject of the role of the CEO does not bring much new knowledge to the research questions which were related to the responsibility in information security and risk management.

The fourth limitation is the fact that the interview could have been more precise regarding information security and collected deeper data and information only about information security. This master's thesis is only scratching the surface of companies' information security and does not receive more details on one subject, information security.

Taking into account the limitations of this study, the future study could research with a larger sample size and with larger companies.

The future study could continue from here where this study ends and then the study would be to research if the awareness has been raised among the CEOs, and if so, how it has occurred.

The selected field of study for this master's thesis was IT. In future studies, this could be compared with other fields and research the difference.

In future studies, the topic of this master's thesis could be researched in more detail and have a simple focus on information security, as this master's thesis had a broad scale to research information security.

REFERENCES

Adams, John & Khan, Hafiz T.A & Raeside, Robert & White, David. 2007. *Research Methods for Graduate Business and Social Science Students*. SAGE Publications India Pvt Ltd. Chapter Research methodology. Retrieved 10.01.2021 from https://sk-sagepub-com.ezproxy.vasa.abo.fi/books/research-methods-for-graduate-business-and-social-science-students/n2.xml#d18.

Ballantyne, Roy & Bruce, Christine. 1994. *Phenomenography: Philosophy and practice.* Centre for Applied Environmental and Social Education Research Faculty of the Education Queensland University of Technology. 7 - 9 November 1994. Publication of the Centre for Applied Environmental and Social Education Research. Retrieved 9.01.2022 from https://eprints.qut.edu.au/216313/1/53908.pdf#page=19.

Bennet, R. & Robson, P. 2004. *The role of boards of directors in small and medium-sized firms.* Journal of Small Business and Enterprise Development, Volume 11, Number 1, 2004. Emerald Group Publishing Limited. Retrieved 14.8.2021 from https://www.emerald.com/insight/content/doi/10.1108/14626000410519137/full/pdf?title=the-role-of-boards-of-directors-in-small-and-mediumsized-firms.

Bojanc R. & Jerman- Blažič, B. 2013. *A Quantitative Model for Information-Security Risk Management.* Engineering Management Journal, 25:2, 25-37. Retrieved 11.9.2021 from https://www.tandfonline.com/doi/pdf/10.1080/10429247.2013.11431972?needAccess=true.

Brink, H.I.L. 1993. *Validity and reliability in qualitative research.* SA society of Nurse Researcher's Workshop. Curationis, Vol 16, NO2. June 1993. Retrieved 30.3.2022 from https://curationis.org.za/index.php/curationis/article/view/1396/1350

Bryman, Alan & Bell, Emma. 2011. *Business research methods.* Third edition. Oxford University Press Inc.

Campbell, G. 2014. *The manager's handbook for business security* (2nd ed.). Waltham, Massachusetts: Elsevier. Retrieved 26.01.2021 from https://ebookcentral-proquest-com.ezproxy.vasa.abo.fi.

Coburn, Andrew. 2018. *Solving Cyber Risk: Protecting Your Company and Society.* John Wiley & Sons, Incorporated. Retrieved 03.03.2021. from https://ebookcentral-proquest-com.ezproxy.vasa.abo.fi/lib/abo-ebooks/reader.action?docID=5614240.

Colwill, Carl. 2010. *Human factors in information security: The insider threat – Who can you trust these days?* BT Security, UK. Laura Pritchard. Published by Elsevier Ltd. Received 24.8.2021. from https://reader.elsevier.com/reader/sd/pii/S1363412710000051?token=6EDE92C3EC4D12504CB0515F2730D0638884AE54EBA326A5B62EED8811B15987878494EAAB3F792B8116A861AFA9B09E&originRegion=eu-west-1&originCreation=20210824125202.

Creswell, John W. 1998. *Qualitative inquiry and research design, Choosing among five traditions.* Sage Publications, Inc.

eDiscovery. *How information governance supports information security.* EpiqSecurity. EpiqGlobal Article. Received 22.02.2022 from https://www.epiqglobal.com/epiq/media/thinking/ediscovery/how-information-governance-supports-information-security.pdf.

Etikan I. & Musa, S-A. & Alkassim R-S. 2015. *Comparison of Convenience Sampling and Purposive Sampling.* Department of Biostatistics, Near East University, Nicosia-TRNC, Cyprus. American Journal of Theoretical and Applied Statistics. Vol. 5, No. 1, 2016, pp. 1-4. Retrieved 30.12.2021 from https://www.sciencepublishinggroup.com/journal/paperinfo?journalid=146&doi=10.11648/j.ajtas.20160501.11

Fenz, S. & Heurix, J. & Neubauer, T. & Pechstein, F. 2013. *Current Challenges in Information Security Management.* Department of Research for consistency, Vienna University of Technology and SBA Research, Department of Science and Technology Management, Xylem Technologies, Department of Research for consistency, Vienna University of Technology and SBA Research, Vienna, Austria. Information Management & Computer Security Vol. 22 No. 5, 2014. © Emerald Group Publishing Limited 0968-5227. Received 13.9.2021 from https://www.emerald.com/insight/content/doi/10.1108/IMCS-07-2013-0053/full/pdf?title=current-challenges-in-information-security-risk-management.

Fitzgerald Todd. 2007. *Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO Must Ask Each Other*. Information Systems Security. Taylor & Francis Group, LLC. Retrieved 19.8.2021. from https://www.tandfonline.com/doi/pdf/10.1080/10658980701746577?needAccess=true.

Gaines-Ross Leslie. 2002. *CEO Reputation: A Key Factor in Shareholder Value*. Burson-Marsteller. Corporate Reputation Review, Volume 3, Number 4. pp. 366–370 Henry Stewart Publications, 1363– 3589. Retrieved 12.11.2021 from https://link.springer.com/content/pdf/10.1057/palgrave.crr.1540127.pdf.

Green Scott. 2004. *Unfinished Business: Abolish the Imperial CEO!* The Journal of Corporate Accounting & Finance. Wiley Periodicals, INC. DOI 10.1002/jcaf.20051. Retrieved 9.11.2021 from https://onlinelibrary.wiley.com/doi/epdf/10.1002/jcaf.20051.

Guthrie, Gerard. 2010. *Basic Research Methods: An Entry to Social Science Research*, chapter: Interviews. SAGE Publications India Pvt Ltd. New Delhi. Retrieved 9.01.2022 from https://sk.sagepub.com/books/basic-research-methods/n11.xml.

Huaman Nicolas, Von Skarczinski Bennet, Stransky Christian, Wermke Dominik, Acar Yasemin, Planck Max, Dreißigacker Arne, Fahl Sascha. 2021. *A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises.* Leibniz University Hannover, CISPA Helmholtz Center for

Information Security, PwC Germany, Institute for Security and Privacy, Criminological Research Institute of Lower Saxony. 30th USENIX Security Symposium. Retrieved 18.8.2021 from https://www.usenix.org/system/files/sec21-huaman.pdf.

Iannarelli, John G. & Michael O'Shaughnessy. (2014). *Information Governance and Security: Protecting and Managing Your Company's Proprietary Information*, Elsevier Science & Technology. ProQuest Ebook Central. Retrieved 27.01.2021 from http://ebookcentral.proquest.com/lib/abo-ebooks/detail.action?docID=1781682.

Merna, Tony & Al-Tani, Faisal. 2008. *Corporate Risk Management.* 2nd edition. John Wiley & Sons, Ltd. Retrieved 25.3.2022 from https://books.google.fi/books?hl=fi&lr=&id=yow0EAAAQBAJ&oi=fnd&pg=PA1&dq=definition+of+corporate+risk+management&ots=GvddJnREUw&sig=LR3-JBv2E_xMENTUdZ2n1S9u4NM&redir_esc=y#v=onepage&q=definition%20of%20corporate%20risk%20management&f=false.

Monakova, Ganna & Brucker, Achim & Schaad Andreas. 2012. *Security and Safety Assets in Business Process.* SAP Research Karlsruhe. SAC'12 March 25–29, 2012, Riva del Garda, Italy. Retrieved 10.8.2021 from https://dl.acm.org/doi/pdf/10.1145/2245276.2232045.

Král David. 2011. *Information security in small and medium-sized companies.* Economic Studies & Analyses / Acta VSFS. University of Finance & Administration. 1/2011, vol. 5. Retrieved 7.8.2021 from https://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=1&sid=2223932e-3474-4cff-83df-8831ccfa9875%40pdc-v-sessmgr02.

Palinkas, Lawrence A. & Horwitz, Sarah M. & Hoagwood, Kimberly & Green, Carla A. & Wisdom, Jennifer P. & Duan, Naihua. 2013. *Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research.* School of Social Work, University of Southern California, Department of Child and Adolescent Psychiatry, New York University, New York, NY, USA. Center for Health Research, Kaiser Permanente Northwest, Portland, OR, USA.

George Washington University, Washington, DC, USA. Department of Psychiatry and New York State Neuropsychiatric Institute, Columbia University, New York, NY, USA. Springer Science+Business Media New York 2013. Published online: 6 November 2013. Retrieved 9.01.2022 from https://link-springer-com.ezproxy.vasa.abo.fi/article/10.1007/s10488-013-0528-y.

Saunders, Mark & Lewis, Philips & Thornhill, Adrian. 2007. *Research methods for business students.* Fourth edition. Pearson Education Limited. England

Sennewald, Charles, A & Baillie, Curtis. 2016. *Effective Security Management.* Butterworth-Heinemann is an imprint of Elsevier The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, UK 225 Wyman Street, Waltham, MA 02451, USA. Retrieved 15.04.2021 from http://ebookcentral.proquest.com/lib/abo-ebooks/detail.action?docID=2147272.

Sattarova, Feruza & Tao-Hoon Kim. 2007. *IT-Security Review: Privacy, Protection, Access Control, Assurance, and System Security.* Hannam University, Department of Multimedia Engineering, 306 791. International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, April 2007. Retrieved 10.8.2021 from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.190.7286&rep=rep1&type=pdf.

Speed, Tyler Justin. (2011). *Asset Protection Through Security Awareness.* Auerbach Publisher, Incorporated. Retrieved 11.02.2021 from http://ebookcentral.proquest.com/lib/abo-ebooks/detail.action?docID=826927

Von Solms, S.H. 2006. Information Security Governance – Compliance management vs operational management. Academy for Information Technology, University of Johannesburg, PO Box 524, Auckland Park, Johannesburg, South Africa. Retrieved 16.9.2021 from https://reader.elsevier.com/reader/sd/pii/S0167404805001057?token=FE0B7379D8DE2A2894C2AF3D9AAB64140F183C1A0695A26701FDC376AED08743A96740C8F1F42E025AD042026FBAACAA&originRegion=eu-west-

1&originCreation=20210916081642.

Yle News. 2020. *Psychotherapy centre's database hacked, patient info held ransom.* Published Yle. Retrieved 7.8.2021 from https://yle.fi/uutiset/osasto/news/psychotherapy_centres_database_hacked_patient_info_held_ransom/11605460.

APPENDIX

Appendix 1. is the research questions to which the participants responded.

About the company:

- Can you tell me in a few sentences what is your company's field of business?
- How many employees are in the company?

Information security

- What does the word information security mean to you?
- How important do you think it is?

- In today's business life, are cyberattacks or data breaches details to consider? Why? Why not?
- Is information security a cost for business?
- Which one do you notify as a greater threat: Cyberattack coming outside of the company or from the inside (e.g. human error from employees)?
- What do you think about training the employees against cyberattacks?
    - How would you do that?
    - Or inform the employees about information security risks?
    - Is this a topic that should be discussed with the employees?
        - what would be the discussion like?

- If a cyberattack or data breach occurred in the company, who do you think is responsible?
    - why?
    - what would be the actions of this person/s?
- Do you as a CEO feel you are in charge of information security?
    - Also if a lack of it existed?
- How do you view yourself as a CEO who is aware of the security department/person?
- If any decisions that you have to make according to information security exist, how are you doing it?

Risk management

- What does risk management mean to you?
- How important do you think it is for the company?
- Do you recognize risk management as an everyday subject in the company?
    - Are all the employees aware of the company's risk management program?
    - Should they be?
- Do you think CEO is the one creating the guidelines for risk management
    - Why? Why not?

- Do you consider risk management in your daily business activities?
- What are the stakeholders' roles in risk management?
- Do you think risk management is governmental ruled and regulated well?
    - Why? Why not?
- If an action is executed by an employee because of an incomplete or non-existent policy and that will affect negative the company who is responsible for it?
    - Why?
- What do you recognize as the greatest assets to the company?
- Do you think all the employees of the company should be aware of the company assets?

CEO and board of directers

- Do you think the size of the company is affecting the role of the CEO?
- Do you seek external expertise as support when no expertise in the company already exists?
- Do you think CEO can be the imperial CEO which means that at the same time be the CEO of the company and the chairman of the board of directors?
- What do you think are the best qualities of a CEO?

Do you have something to add or comment on here at the end?