UNIVERSITY OF TURKU

ABSTRACT

	Bachelor's thesis
X	Master's thesis
	Licentiate's thesis
	Doctoral dissertation

Subject	International Business	Date	30.11.2020
Author	Jonna Reilimo	Number of pages	91 + appendices
Title	Preparedness against cybersecurity threats- A study of SMEs in the Nordic region		
Supervisors	Ph.D. Eriikka Paavilainen-Mäntymäki & Ph.D. Milla Wirén		

Along with the advantages and opportunities of the use of technological solutions, new threats have risen in the form of cyber threats. The importance of cybersecurity has grown and as opposed to general misconceptions, this research indicates that even SMEs are likely to encounter cyber risks and the consequences might include significant monetary losses. Nevertheless, according to previous research and empirical findings, the level of cybersecurity in SMEs seems to generally be rather low. Therefore, this research was directed to examining why the level of cybersecurity varies in Nordic SMEs and how it could be improved.

The theoretical framework used in this research concentrated on operational risk management, cyber risk management and challenges that SMEs encounter regarding cybersecurity. These theories were utilized later in the analysis of applying the theoretical framework with the use of empirical findings to the context of SMEs. The research was conducted qualitatively by conducting semi-structured interviews with six industry experts.

The empirical findings show that it is rather common that also SMEs nowadays encounter cyberattacks due to e.g. automatization, simplicity of cyberattacks and the fact that SMEs are often easier targets. In addition, study's results showed three categories of most common cyberattacks for SMEs: extorsion attacks, attacks that aim to steal sensitive data, and attacks that exploit the target company's IT resources. In addition, the study's results indicated that the most common reasons for why SMEs might not have prepared for cyberattacks include the lack of awareness, limited financial and human resources, and lack of cybersecurity governance. Moreover, the study's results indicated different normative suggestions on how to improve the level or cybersecurity in Nordic SMEs. Strategical and operational level suggestions followed the theoretical framework by adapting the different phases of cyber risk management to the context of SMEs. The technical level suggestions, on the other hand, presented more practical tools on how to improve the level of cybersecurity in Nordic SMEs.

These results of the study were used to apply the existing theories in cyber risk management to suit the context of SMEs thus, representing the theoretical contribution of the research. In addition, the results regarding the threats these Nordic SMEs might encounter and how they could improve their cybersecurity can be regarded as practical contribution of this research.

Key words	Cybersecurity, SMEs, cyberattack, cyber risk, operational risk management, cyber risk management, cyber-resilience.

TURUN YLIOPISTO

TIIVISTELMÄ

	Kandidaatintutkielma
X	Pro gradu -tutkielma
	Lisensiaatintutkielma
	Väitöskirja

Oppiaine	Kansainvälinen liiketoiminta	Päivämäärä	30.11.2020
Tekijä	Jonna Reilimo	Sivumäärä	91 s. + liitteet
Otsikko	Valmius kyberturvallisuusuhkia vastaan- Tutkimus pohjoismaisista pk-yrityksistä		
Ohjaajat	Ph.D. Eriikka Paavilainen-Mäntymäki & Ph.D. Milla Wirén		

Teknologian ja sen tuomien hyötyjen ja mahdollisuuksien mukana yritykset ovat kohdanneet myös uusia uhkia. Kyberuhkien vuoksi kyberturvallisuuden merkitys on kasvanut ja tämä tutkimus osoittaa, että vastoin yleisiä väärinkäsityksiä, myös pk-yritykset saattavat hyvin todennäköisesti joutua kyberhyökkäysten kohteiksi ja seuraukset saattavat johtaa merkittäviinkin taloudellisiin menetyksiin. Siitä huolimatta tutkimuksen tulokset sekä aiempi aiheesta tehty tutkimus viittaa siihen, että kyberturvallisuuden taso pk-yrityksissä on yleisellä tasolla suhteellisen matala. Tästä syystä tämän tutkimuksen aiheena on tutkia syitä kyberturvallisuuden tasojen vaihtelulle pohjoismaisissa pk-yrityksissä sekä mahdollisuuksia, miten kyberturvallisuuden tasoa voisi pk-yrityksissä parantaa.

Tutkimuksessa käytetty teoreettinen viitekehys koostuu operatiivisen riskijohtamisen sekä kyberriskijohtamisen teorioista. Lisäksi teoreettinen viitekehys sisältää olemassa olevan kirjallisuuden tutkimustuloksia siitä, millaisia haasteita pk-yritykset kohtaavat kyberturvallisuuteen liittyen. Tätä teoreettista viitekehystä on lisäksi käytetty tutkimustulosten analyysissä. Tutkimustulosten analyysin avulla teoreettista viitekehystä on sovellettu sopimaan pk-yritysten kontekstiin. Tutkimus on toteutettu käyttäen kvalitatiivista menetelmää ja tutkimuksen data on kerätty tekemällä kuusi puolistrukturoitua haastattelua kyberturvallisuusalan asiantuntijoiden kanssa.

Tutkimustulokset osoittavat, että on suhteellisen yleistä, että myös pk-yritykset joutuvat kohtaamaan kyberhyökkäyksiä. Syinä tähän ilmiöön olivat esim. hyökkäysten automatisointi, hyökkäysten helppous ja se, että pk-yritykset ovat usein helppoja kohteita hyökkääjille. Lisäksi tulokset indikoivat kolmea kyberhyökkäysten kategoriaa, joita pk-yritykset saattaisivat kohdata: kiristys hyökkäykset, hyökkäykset, joiden tavoitteena on varastaa arkaluontoista dataa sekä hyökkäykset, joiden tavoitteena on hyväksikäyttää kohteen tietoteknisiä resursseja. Lisäksi tulokset osoittivat, että pk-yritysten kyberturvallisuus saattaa olla heikolla tasolla, jos tietoisuus ei ole riittävällä tasolla. Lisäksi tekijät, kuten rajalliset taloudelliset ja henkilöstöresurssit sekä kyberturvallisuuden vastuuttamisen sekä johtamisen puute saattavat tutkimustulosten mukaan vaikuttaa alhaiseen varautumisen tasoon. Lisäksi tulokset tuottivat erinäisiä ehdotuksia sille, kuinka pohjoismaisten pk-yritysten kyberturvallisuutta voisi parantaa.

Avainsanat	Kyberturvallisuus, tietoturva, kyberhyökkäys, Pk-yritykset, kyberriskijohtaminen
Muita tietoja	-

UNIVERSITY OF TURKU
Turku School of Economics

PREPAREDNESS AGAINST CYBERSECURITY THREATS

A study of SMEs in the Nordic region

Master's Thesis
in international business

Author:
Jonna Reilimo

Supervisors:
Ph.D. Eriikka Paavilainen-Mäntymäki
Ph.D. Milla Wirén

30.11.2020
Turku

TABLE OF CONTENTS

APPENDICES

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND KEY TERMS

Artificial intelligence (AI) is "an area of study in the field of computer science. Artificial intelligence is concerned with the development of computers able to engage in human-like thought processes such as learning, reasoning, and self-correction." (Kok et al. 2009)

Coronavirus disease (COVID-19) "is the infectious disease caused by the coronavirus, SARS-CoV-2, which is a respiratory pathogen. WHO first learned of this new virus from cases in Wuhan, People's Republic of China on 31 December 2019." (Coronavirus disease (COVID-19)). In March 2019 the World Health Organization declared the disease as pandemic (Coronavirus confirmed as pandemic by World Health Organization).

Cyberattack is "an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm." (Merriam-Webster)

Cyberattack vector "is a path or means by which an attacker can gain unauthorized access to a computer or network to deliver a payload or malicious outcome." (What is an Attack Vector? Common Attack Vectors)

Cyber risk is "a risk caused by a cyber threat" (Refsdal et al. 2015, 33). It "is an operational risk that involves direct or indirect damage by economic agents as a result of their operation in cyberspace" (Klapkiv & Klapkiv 2018, 243).

Cybersecurity is "the practice of protecting systems, networks, and programs from digital attacks." (What Is Cybersecurity?)

Cyber threats "encompass sophisticated malicious software, disruptive activity by online activists and nationalist groups, and even organized crime and electronic cyber espionage activities." (Nam 2019, 2)

Denial-of-service attack (DoS) "occurs when someone attempts to overload a system through an online connection in order to force it to shut down." (Rittinghouse & Hancock 2003, 77)

General Data Protection Regulation (GDPR) "sets out detailed requirements for companies and organisations on collecting, storing and managing personal data. It applies both to European organisations that process personal data of individuals in the EU, and to organisations outside the EU that target people living in the EU." (Data protection under GDPR)

Internet of things (IoT) is "a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies." (Wortmann & Flüchter 2015, 221)

Multinational Corporation (MNC) (Merriam-Webster)

Phishing is "a scam by which an Internet user is duped (as by a deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly." (Merriam-Webster)

Ransomware is "a type of malicious software designed to block access to applications or files on a computer system until a sum of money is paid". (Oxford Learner's Dictionary)

Return on investment (ROI) is a measure to calculate the cost-efficiency of an investment

Small and medium-sized enterprise (SME) is a company with staff headcount under 250 and turnover less or equal to €50m or balance sheet total less or equal to €43m. (What is an SME?)

Virtual private network (VPN) is "a private computer network that functions over a public network". (Merriam-Webster)

1 INTRODUCTION

1.1 The rising concern of cybersecurity

The contemporary business world is driven by technology. Technology can now be seen everywhere, and the phenomenon has rooted deeply into societies. Thus, we might not even realise how much technology actually affects our lives. Even in normal conditions, companies rely heavily on technological solutions in their day-to-day operations and suddenly, in 2020, the technological dependence rose to everyone's attention as the world pandemic COVID-19 drove millions of people worldwide to work from home. By affecting the world economy, this worldwide health crisis has even more emphasized the fact that without smart and optimal use of technology-based operations, companies might easily lose their competitive advantage and even cease to exist. The advantages and opportunities that the rapid technological development has created in the past years are inarguable and the technological improvement has disrupted the way we do business. However, the growing dependence and reliance on technology has created new threats for businesses as well. The risks caused by cyber incidents are high even in normal conditions and due to the rapid expansion in remote working, cyber criminals have now even greater feasibility to exploit the deficiencies in cybersecurity. Hence, cyber risks should not be bypassed even in normal conditions, let alone during crisis situations. Thus, due to the sudden increase in remote work after the spreading of COVID-19 pandemic, the importance of cybersecurity has grown even higher.

Allianz Group publishes yearly a report called Allianz Risk Barometer which reports the top business risks for the year ahead and beyond. The report is written using a survey method and in the 2019 report they had collected 2,415 respondents from 86 countries representing 22 industry sectors (Allianz Risk Barometer 2019, 3). In the Allianz Risk Barometer 2019 cyber incidents rank second in the list of top ten global business risks, and first in the list of top five risks for SMEs[1] (Allianz Risk Barometer 2019, 22). Thus, it is evident that while the world is rapidly moving even more towards technologically based solutions and operations, businesses, even smaller ones, are increasingly more vulnerable to new threats rising from cybersecurity issues.

[1] The Allianz report has defined small enterprise companies as companies with annual revenue under € 250m. In this report, the term SME refers to companies with annual revenue under € 50m. Hence, the list of the top five risks for SMEs might not be exactly the same if we would only consider companies with revenue under € 50m. However, the point remains the same: cyber threats are a major risk for any sized company.

In addition, following the increase in globalization, companies' cloud service usage and outsourcing, cyberattack vectors (i.e. the means of paths by which an attacker can access a network or a computer) have expanded. The expansion of these cyberattack vectors has increased the possibilities of attackers exploiting these new opportunities of accessing companies remotely. Moreover, due to these large attack vectors, SMEs often work as the "weakest link" in the network of possible targets (Tawileh et al. 2007, 332). Thus, an SME might be the easiest point of entry into the system for an attacker. Hence, Tawileh et al. (2007, 332) argue that special attention ought to be paid to this weakest link of the network: SMEs.

There are numerous motives for cyberattacks depending on the attacker's interests. The most common motives are often either financial or related to cyber-espionage (Getting defensive: how businesses can guard against cyberattacks). Additionally, motives for cyberattacks can include e.g. testing the cyber warfare capacity, searching and mapping possible targets, revenge, attacker's renown or status seek, ideological or political motives etc. (Johnson 2016, 129-136). Ransomwares, which are discussed more in depth later in this paper, represent an example of cyberattacks which are driven by financial motives since the attackers typically threaten the victims to pay ransoms in the form of crypto currencies. Cyber-espionage as a motive, on the other hand, is directed towards accessing sensitive data. Perhaps the most commonly known example of a cyberattack driven by cyber-espionage is phishing. Phishing is known as the practice of accessing and stealing sensitive data through the method of fraudulent communication, most commonly, emails. By accessing sensitive data, the attacker might gain access for instance to passwords, bank and credit card details, pricing information, sensitive R&D information or client data (Johnson 2016, 65, 130). Hence, these motives can also overlap. For instance, by accessing sensitive data through cyber-espionage, the attacker might be able to use the data to achieve financial gains.

Regardless of the motives behind cyberattacks, often only large-scaled cybercrimes make the news headlines. However, there are additionally many other mundane threats and weaknesses with technology-based systems. IT malfunctions, for instance, can create major losses for any sized company if it is unable to operate normally after a cyber incident. Hence, a company's potential vulnerability to cyberattacks poses a major threat for the company regardless of its size. In his article, Lepistö (2019) has interviewed IBM Finland's cybersecurity country manager Juha Kolehmainen. Kolehmainen mentions that cyber criminality has grown into a billion-euro business and is ought to soon rise above

illegal drug trading in terms of value. Kolehmainen additionally mentions that a study for IBM concludes that it takes approximately 200 days for companies to notice a cyberattack and the losses can thus, be over a million euros for a company under an attack. Hence, it is evident that the risks related to cyberattacks are significant.

The level of concern regarding companies' risks is often proportional to the level of potential financial impact the risk might have to the company. Thus, it is evident that cyber risks have become major concerns for many IT executives. As mentioned above, the costs of facing a cyberattack can rise to significantly high levels. The average cost of a malware infection for an organization was accounted for $235.000 at the time Rees et al. (2011, 493) wrote their article and the costs have only gone up as Lepistö (2019) mentioned. According to the Allianz Risk Barometer 2019 (2019, 12), the average insured loss from a cyber incident now exceeds two million euros. For SMEs the costs are naturally lower but can still put the company's future at a great risk. The insurance company Hiscox reported that in 2019 the mean cost of cybersecurity incidents for small companies was $14,000 and for medium-sized companies $184,000[2] (Hiscox Cyber Readiness Report 2019, 6). Hence, the financial effect of cyberattacks and -incidents seems to be significant whether the company is small, medium-sized or large especially when mirroring the financial losses for SMEs against their annual revenues.

Additionally, according to the article by Lepistö (2019), the costs from cyberattacks have risen 20% over the past year in the Nordic countries. This indicates another reason why the subject is relevant and worth further investigation. In his article, Lepistö has also interviewed a professor from Aalto University, Jarno Limnéll, who is an expert in the field of cybersecurity. Regarding the rising trend of cyberattacks, Limnéll mentioned that the preparedness of companies in Finland against cyberattacks varies significantly. In fact, Kaušpadienė et al. (2019, 980) additionally state that only 9% of SMEs seem to have an organizational culture concerning cybersecurity. Furthermore, it could be argued that many SMEs are unprepared for cybersecurity risks due to either unawareness or conscious decision to neglect and ignore these cybersecurity issues (Yannakogeorgos & Lowther 2013, 9). The book by Yannakogeorgos and Lowther (2013), however, does not indicate which of these two reasons are more common among SMEs, nor has it gone further into investigating the plausible reasons behind SMEs' tendencies to consciously ignore cybersecurity issues.

[2] The report is using the EU definition of SMEs.

In their article, Rubio et al. (2019), have studied different cyber threats and different methods used to proactively prepare for such threats. The article (Rubio et al. 2019, 10), furthermore, mentions that there exists a research gap for how companies have integrated these methods in their business strategies. Kabanda et al. (2018, 269) also refer to the same research gap that the existing literature is limited concerning cybersecurity in the context of SMEs. Hence, regardless of the evident and plausible risks from cyberattacks, there seems to be limited research available on the cybersecurity levels and practices in the context of SMEs.

1.2 Research objectives and structure of the study

World's dependence on technology is growing along with the advancements in technology, artificial intelligence (AI) and Internet of things (IoT). Companies, even SMEs, are unlikely to survive without using technology and thus, vulnerabilities regarding cybersecurity are increasing in a fast pace. However, companies still seem to have very different levels of preparedness against cyber threats, as discussed in the previous subchapter. Kurpjuhn (2015, 5) mentions in his article that cybersecurity risks are equally significant for SMEs as they are for larger organizations. In addition, many news articles refer to the same reality that SMEs are at an equal risk of facing cyberattacks as are larger companies. In fact, the news channel CNBC (Steinberg 2019) reported study results by Accenture that 43% of online cyberattacks are now targeted towards small businesses and only 14 % of these businesses have prepared against cyberattacks. Hence, it is quite evident that the size of the company is not nowadays associated with the likeliness of becoming a target of a cyberattack. In addition to the size of the company, it also seems to be irrelevant whether the company works in private or public sector. Nam (2019, 2) concludes in his article that the scope of cyber threats remains the same regardless of the target being a private or public organization.

Due to the apparent differences in the level of preparedness against cyber threats and the limited research around the subject in the context of SMEs as discussed in the previous subchapter, the aim of this research is to study the state of cybersecurity preparedness in Nordic SMEs. Particularly, the research aims to examine why SMEs' preparedness against cybersecurity threats is at such a low level (see, for example, Kaušpadienė et al. 2019, 980; Steinberg 2019) even though these cyber threats seem to present a significant risk for SMEs as well. In addition, the aim is to investigate whether there would be room

for improvements concerning the cybersecurity preparedness of these SMEs. To conclude the aim of the research explained above, the research problem has been formulated as follows:

The state of cybersecurity in Nordic SMEs: why it varies and are there room for improvements?

In could be assumed that attributes such as attitudes, resources and awareness of cybersecurity issues might differ rather considerably between different economies around the world. Therefore, the study's focus has been narrowed down to companies operating in the Nordics for feasibility purposes. In order to facilitate the process of examining the research problem presented above, the following three research questions have been utilized in the research process:

(1) What are the cybersecurity risks for SMEs operating in the Nordic countries?
(2) Why SMEs operating in the Nordic countries generally have not prepared against cyber threats?
(3) How could SMEs prepare for cyber threats?

These three research questions have been modified during the research process. In the beginning of the research process, the research questions were more directed towards examining how Nordic SMEs have prepared against cyber threats and what motivates them to prepare or why they would not have prepared against cyber threats. However, as previous literature became more familiar and as the research process continued to the data collection phase, it quickly became obvious according to previous research (see, for example, Kaušpadienė et al. 2019, 980; Steinberg 2019) and the interviewed industry experts that generally SMEs in the Nordics have not prepared against cyber threats if the parameters are limited to the EU's definition of SMEs. Therefore, the research questions were modified as presented above. The following quote from the empirical data gathered demonstrates the reason for why the research questions were modified:

> *"Okay, well I can already tell you quite frankly that in that category [EU's definition of SMEs] none of the companies have any kind of cybersecurity strategy. It would be extremely rare that with those parameters [EU's*

> *definition of SMEs] any company would have any kind of [cybersecurity] strategy or even anyone responsible for it."* (Global Technical Director and a "professional hacker")

However, the current level of preparedness for cyber threats in SMEs does not diminish the importance of cybersecurity even in the context of these companies. The quote presented below illustrates how even SMEs would need to consider these cyber threats taking into account the context they are operating in:

> *"Every company needs to adopt an IT security position which is adequate to its size, operations and risk profile and invest in technological security solutions, proper backup mechanisms and staff training. The last aspect is possibly the easiest one to miss but is equally important, especially for small- and mid-sized enterprises."* (Allianz Risk Barometer 2019, 13)

Nevertheless, regardless of the importance of cybersecurity, based on previous research and industry experts' insights it seems that in the Nordics, generally SMEs have not prepared for these risks. Hence, the aim is to study why the state of preparedness is at this level and how these Nordic SMEs could improve their cybersecurity.

As mentioned earlier, for the sake of feasibility and in order to fill a gap in the existing research, the research problem has been focused on SMEs operating in the Nordic area. In this research, SMEs refer to the EU's definition that the company's staff headcount is less than 250 and its turnover is less or equal to € 50m or its balance sheet total is less or equal to € 43m (What is an SME?). This scope was additionally taken due to the fact that larger companies have already been under research regarding cybersecurity preparedness issues by different actors such as academic researchers and consulting companies (see, for example, The future of cyber survey 2019 by Deloitte). Even though the study has been limited to examining companies operating in the Nordic region (Finland, Sweden, Norway, Denmark and Iceland), the results have a special emphasis on Finland since most of the interviewees had the most experience from the Finnish markets.

Lastly, it is important to note that the study has not been constrained by limiting the scope of the research to specific industries since it seems that the cybersecurity preparedness varies generally in the market as a whole. Thus, the research problem has been developed considering all SMEs regardless of the industry they operate in.

Nevertheless, it could be presumed that SMEs working in some industries such as the IT-industry might be more aware of the risks and thus better prepared. Additionally, some industries might have stricter legislative obligations and thus, the preparedness ought to be at a higher level than in other industries. Moreover, it could be speculated that some industries are more vulnerable for cyber threats than others, for instance, due to higher levels of technology usage. However, in order to avoid any assumptions, the study was made without limiting the scope to any specific industry.

In addition to tightening the research gap from the scientific perspective, the aim is to provide normative information for companies as well. Thus, the research is aimed to provide valuable information about the cybersecurity in general and about the different cyber threats Nordic SMEs might encounter. Especially finding answers to the third research question of how SMEs could better prepare against cyber threats, is hoped to benefit SMEs working in the Nordic region by providing practical insights from the industry experts. These scientific and practical contributions of the research are discussed further in chapter six.

For the sake of coherence, it is important to additionally define some of the main concepts used throughout the text. In addition, the reader can return to the glossary of the main concepts and abbreviations at the beginning of this paper, if needed. The most relevant concepts in this paper include at least cybersecurity, cyberattacks, cyber threats, and cyber risks. First, cybersecurity can be defined as "the practice of protecting systems, networks, and programs from digital attacks" (What Is Cybersecurity?). These "digital" or cyberattacks, on the other hand, "aim to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data" (What is a Cyber Threat?). In this paper, a cyber threat, on the other hand, can be considered as a malicious attempt to orchestrate a cyberattack. Although, cyber threats usually are malicious, there can also be non-malicious cyber threats and cyber threats that have both malicious and non-malicious motives (Refsdal et al. 2015, 33-34). Another noteworthy feature of cyber threats and cyberattacks is that they can rise internally from the organization or externally from unknown parties accessing the company remotely. Thus, the potential threat sources can locate anywhere in the world (Refsdal et al. 2015, 33). Finally, cyber risks are risks caused by cyber threats (Refsdal et al. 2015, 33). Other main concepts used in this paper are defined as they arise. Moreover, the above-mentioned glossary offers the reader additional support for following the paper.

The structure of the paper has been divided into seven chapters. This first chapter introduced the subject under investigation and motives for conducting the research as well as the objectives of the research. Chapter two presents the state of the world cybersecurity at the time this paper was written. Chapter three introduces previous literature that has been used as a theoretical framework for the research. The section of previous literature is further linked in the analysis of the study's results and hence, is an integral part of chapter five. The methodology used to conduct the research has been explained further in chapter four. Chapter five, on the other hand, introduces the results gathered from the data collection and the analysis of the study's results. Chapter six draws conclusions on the theoretical and practical implications of the research and proposes suggestions for further research. Lastly, chapter seven summarizes the research conducted and its main findings.

2 THE STATE OF WORLD'S CYBERSECURITY

2.1 Some notable cyberattacks

To illustrate the nature and the magnitude of cyberattacks, this subchapter will introduce the most disruptive global cyberattacks from the past years. It remains important to notice that while these most disruptive cyberattacks might get the most media coverage, the number of cyberattacks worldwide is estimated to amount approximately to 350,000 attacks per year (Allianz Risk Barometer 2019, 12). Therefore, the cases ending up in the news headlines, can be seen merely as drops in the ocean. It is also important to notice that even though these major attacks often end up in the news headlines, smaller companies can still face similar attacks even if the economic losses might not be as large as with these cases.

In May 2017 a ransomware attack globally known as the WannaCry Ransomware hit computers across globe. According to Oxford Learner's Dictionary a ransomware is defined as "a type of malicious software designed to block access to applications or files on a computer system until a sum of money is paid". The WannaCry ransomware hit hundreds of thousands of computers worldwide. Compared to other ransomware types, the WannaCry was exceptionally dangerous due to its ability to spread itself across an organization's network exploiting Windows vulnerabilities (What you need to know about the WannaCry Ransomware). After hitting a computer, the WannaCry ransomware demanded the user to pay USD 300 in bitcoins and doubled the amount after three days if the ransom was not paid. Finally, the WannaCry ransomware threatened to delete all the encrypted files after seven days if the ransom would not be paid. The WannaCry ransomware awakened the business world and highlighted the importance of back-ups since the recovery of the encrypted files seemed to otherwise be impossible. Much like WannaCry, another ransomware hit the world in June 2017. The Petya ransomware also demanded USD 300 to be paid in bitcoins in order to recover the files it had encrypted. However, Petya ransomware did not just encrypt files but also overwrote and encrypted master boot records (Petya ransomware outbreak: Here's what you need to know).

In addition to ransomwares, data breaches have been tormenting businesses around the world in the past few years. Equifax, Facebook and Uber are all examples of companies that have had to recover form large data breach crises. In March 2017, personal data of at least 145.5 million people was stolen from a credit reporting agency Equifax

due to a number of security lapses in the company (Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach). Equifax assesses the financial stability of nearly every US citizen and thus, the data breach extended to many individuals. Additionally, in September 2018, Facebook faced a large data breach affecting nearly 50 million users due to software flaws in the company's systems (Facebook Security Breach Exposes Accounts of 50 Million Users). In November 2017 Uber announced that the company had faced a data security incident. In the data breach, the hackers had downloaded data containing names and driver's license numbers of approximately 600,000 drivers and personal information (names, phone numbers and e-mail addresses) of 57 million Uber users around the world (2016 Data Security Incident). According to the Uber's press release (2016 Data Security Incident), the attackers were able to access the data through a third-party cloud-based service that Uber uses. In addition to these three example cases, one of the largest data breaches on record at the time of writing this paper was detected in November 2018, when the hotel group Marriott faced a massive data breach affecting over 500 million customers due to an unauthorized access to the network (Marriott Breach -- What Happened, How Serious Is It And Who Is Impacted?). The compromised data of nearly 380 million individuals (Allianz Risk Barometer 2019, 12) included highly personal information such as passport numbers, payment information, names, addresses, phone numbers and e-mail addresses (Marriott Breach -- What Happened, How Serious Is It and Who Is Impacted?). The cost of Marriott's data breach is estimated between USD 200mn and USD 600mn (Allianz Risk Barometer 2019, 12).

Even though these massive cyberattacks often receive more media coverage, the cybersecurity threats remain the same regardless of the company's size even if the monetary costs will not escalate into same magnitudes as in the case of Marriott, for instance. These above-mentioned examples, however, offer an insight into the nature and consequences of cybersecurity failures. Throughout this paper, cyberattacks refer to these types of cybercrimes, such as ransomwares and data breaches which often lead to monetary losses such as fines and penalties.

2.2 Rising regulation: GDPR

The rising number of data breaches has driven the political discussion towards nation states' and supranational entities' responsibility to protect citizens' personal data. Thus,

nation states and supranational entities have started to create laws and regulations which now bind companies to protect the data they gather and hold. Hence, a large portion of the monetary costs that a company could face in case of a data breach, can come from fines and penalties of neglecting to follow these laws and regulations.

Since the focus of this study is to look more closely at SMEs operating in the Nordic countries, the most critical regulation these companies face is the General Data Protection Regulation (GDPR) that entered force in May 2018. The GDPR has increased both consumers' privacy rights and regulators' enforcement powers in the EU. After the GDPR enforcement, companies are now obligated to pay more attention to holding inclusive and up-to-date documentation, detecting and preventing cybersecurity risks, developing internal processes, and following legal guidelines (Tietosuoja-asetus). Hence, accountability has become crucial when processing or controlling personal data. However, designating a data protection officer is not a legal obligation for every company[3] and thus, might affect cybersecurity procedures in SMEs.

By neglecting to comply with the GDPR, companies face a significant risk of economic sanctions in the form of fines and penalties. In fact, the fines for not complying with the GDPR can increase up to EUR 20m or 4% of the company's turnover whichever is higher (Council of the European Union 2016). Even with minor violations, the fines can increase up to EUR 10m or 2% of the company's annual turnover whichever is higher (Council of the European Union 2016). Under the GDPR, companies that control personal data are, additionally, obligated to report all data breaches to the supervisory authority within 72 hours from when the breach has been detected (Council of the European Union 2016). Moreover, if the breach is likely to result in a high privacy risk for individuals, the individuals or data subjects must also be notified about the breach (Council of the European Union 2016). Thus, due to increased transparency requirements from the GDPR towards individuals' data protection, companies have to consider reputational risks in addition to the economic risks that might arise form fines and penalties.

Penalties and fines from laws and regulations are, however, not the only monetary concern companies have after a data breach. Consumer class actions have become more and more common and have now started to spread from US to Europe (Allianz Risk

[3] Designating a data protection officer is obligatory for companies when the "core activities of the [data] controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale" (Lex Access to European Union law).

Barometer 2019, 13). The case of British Airways data breach can be seen as an example of a consumer class action in Europe. British Airways discovered a data breach in September 2018 where approximately 500,000 customers' personal data was compromised. Under the GDPR regulation, British Airways is facing a GBP 183m fine (British Airways faces record £183m fine for data breach) and additionally, the data breach has triggered class actions against the airline (Allianz Risk Barometer 2019, 13). Hence, the monetary costs of the incident can accumulate to a much higher amount than the original fine.

Even though it might be presumed that class actions would be a higher risk for larger companies such as British Airways, it is still vital even for SMEs to consider the legal requirements that come with controlling and processing personal data. Many SMEs use this type of data in one way or another and thus, are often obligated to follow the GDPR whereas any larger company is. Therefore, even without an official nominated data protection officer, taking responsibility for compelling with the regulation can be vital for a company's survival.

2.3 Cybersecurity and other world threats: Covid-19

Cyber threats arise when cyber criminals find possibilities to exploit vulnerabilities in IT infrastructures. These vulnerabilities might easily develop as a consequence of company's battle against another threat. Thus, cybersecurity should not be regarded as separate phenomenon but rather as a contextual issue that is related to almost all other company operations. An example of the interconnectivity can be seen when the world had to prepare for the battle against a new world pandemic Covid-19. As a consequence of the fight against the pandemic, millions of people were recommended to work remotely from their homes to prevent the spreading of the virus (Heikkilä 2020). Consequently, the sudden increase in remote working has created new opportunities for cyber criminals to detect vulnerabilities in network systems and in fact, security professionals have seen a surge in cyberattacks exploiting Covid-19 (Sangster 2020). Phishing attempts have increased and it is even more vital for companies to educate their staff to be even more cautious when working from home offices.

In addition to phishing attempts, another significant cybersecurity threat arises if an employee is using a personal computer, has an unsecured Wi-Fi connection, or is using a

public Wi-Fi connection for business purposes (Heikkilä 2020). A significant threat in remote working, therefore, comes from employees using personal computers, home network connections or public Wi-Fi connections. Thus, it is vital for cybersecurity that Wi-Fis and routers are secured using strong passwords. Hence, especially if VPN connections are not used, companies ought to remind their staff that remote work comes with a responsibility to ensure that these passwords are used and that they are strong (Hyppönen 2020). Additionally, F-secure's Chief Research Officer Hyppönen (2020) reminds that the employers need to pay even more attention to monitoring and enabling operation system updates and application updates.

Since the spreading of the Covid-19 started quite rapidly, companies had to enforce agile decisions and transform business strategies rather quickly. In addition to rapid, agile strategy decisions, companies have had to accommodate their risk analyses to suit the situation and thus, cybersecurity ought to be an integral part of those analyses. The rapid changes create a challenge for companies and at the time of writing this paper, it remains to be seen how much cyber criminals end up exploiting the new opportunities due to a worldwide crisis situation and how well companies can survive from the situation and all the new risks it has created in terms of cybersecurity and cyber-resilience.

3 THEORETICAL FRAMEWORK

3.1 Operational risk management

Cybersecurity is essentially a part of an organization's risk management strategy. In order to examine the research problem and find answers to the research questions posed earlier in chapter 1.2, it is important to understand in a wider sense how companies can identify risks and how these risks can be managed. Thus, this third chapter begins with introducing a more general theoretical framework of operational risk management. In chapter 3.2 the scope is narrowed more specifically down to cyber risk management. Hence, the structure of the theoretical framework is intended to start from a wider perspective to understand the generalities of risk management strategies and then narrowing down the context more specifically to cybersecurity. Chapter 3.3 focuses on the challenges SMEs encounter in terms of cyber risk management. Finally, a theoretical synthesis from the perspective of SMEs has been drawn in chapter 3.4. The theoretical synthesis in chapter 3.4 has been constructed iteratively based on the empirical findings and the theories presented in chapters 3.1-3.3.

There are many different definitions for risk and risk management (Purdy 2010, 881). Thus, the International Organization for Standardization (ISO) has introduced one vocabulary aiming to achieve consistency and reliability (Purdy 2010, 881). This publication, ISO 31000:2009, is widely recognized and introduces risk as neither positive nor negative but rather the concept emphasizes that consequences of risks "may vary from loss and detriment to gain and benefit" (Purdy 2010, 882). As opposed to the ISO 31000:2009 publication's definition of risk, Pinto et al. (2015, 4-5), for instance, have defined risk as potential events with undesirable consequences. Due to the scope of the research, in this paper, risks are also considered more as events that generate negative outcomes for companies. However, it is worthwhile to recognize that in some contexts and publications, risks can also refer to events that result in positive consequences.

The Basel Committee on Banking Supervision (2011, 3) has defined operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." In order to get a deeper understanding of operational risks, they are often categorized or classified. There are various ways a company can categorize operational risks. Pinto et al. (2015, 10-13), for instance, have introduced three different ways for this categorisation. These ways for categorization have been

summarized below in figure 1. First, operational risks can be categorized by the elements that constitute the system and its environment (people, processes, information, materials, machines and external events). Second, operational risks can be categorized by the origin of the events (organisational, technical, social, political and environmental). The third option could be to categorize operational risks by the consequences the risk has for the company (safety, financial, legal and security). Whichever classification method is used, it is important to recognize that cyber risks can be highly interdependent and thus, it could be argued that cyber risks could be present in almost every category. This argument will be discussed further in chapter 3.2.

Figure 1 Categorization of operational risks (Pinto et al. 2015, 10-13)

The definition and categorization of risks and more specifically, operational risks, give a better understanding to the theoretical framework of operational risk management. The ISO 31000:2009 publication defines risk management as the "process of optimization that makes the achievement of objectives more likely" (Purdy 2010, 882). Moreover, operational risk management can be considered as the "the design and control processes that will affect operational risks" (Pinto et al. 2015, 10). Therefore, operational risk management often begins with recognition. In order to detect any operational risks, the company has to, thus, recognize its goals and objectives, interrelationships among elements of a system and system boundaries (Pinto et al. 2015, 7-8; Ilmonen et al. 2010,

21-22). Recognising goals and objectives allows the company to later determine whether events are intentional or not and whether the consequences are undesirable or not (Pinto et al. 2015, 7). The classification of events' consequences, therefore, determines whether the company considers the event as a risk. Furthermore, the classification of events' intentionality can further assist when the company needs to assess the risks' mitigation strategies. This is discussed later in this chapter when the process of operation risk management is covered more thoroughly.

Pinto et al. (2015, 15-16) have identified three stages in operation risk management: risk identification, assessment and mitigation. Most risk management theories follow more or less the same stages although different authors might use different concepts for each stage (see, for example, Ilmonen et al. 2010, 31; Lam 2014, 37; Refsdal et al. 2015, 36; Haimes 2016, 214; Limnéll et al. 2014, 110). The first stage of risk identification includes an analysis of what essentially can go wrong. Identifying risks is essential for a company in order for it to protect itself against possible threats. Secondly, risk assessment contains a deeper analysis of the likelihoods, causes, and consequences of the risks identified in the first stage. Thirdly, risk mitigation or treatment includes planning on what risk management strategies are used and how the identified risks are controlled. In addition to these three stages, most risk management theories include auditing and regular re-assessment of the risk management strategy (see, for example, Ilmonen et al. 2010, 31; Refsdal et al. 2015, 45-46). These operational risk management stages and their main characteristics are synthesized form previous literature below in figure 2. Then, each stage is discussed further to grasp a deeper understanding of the process of operational risk management.

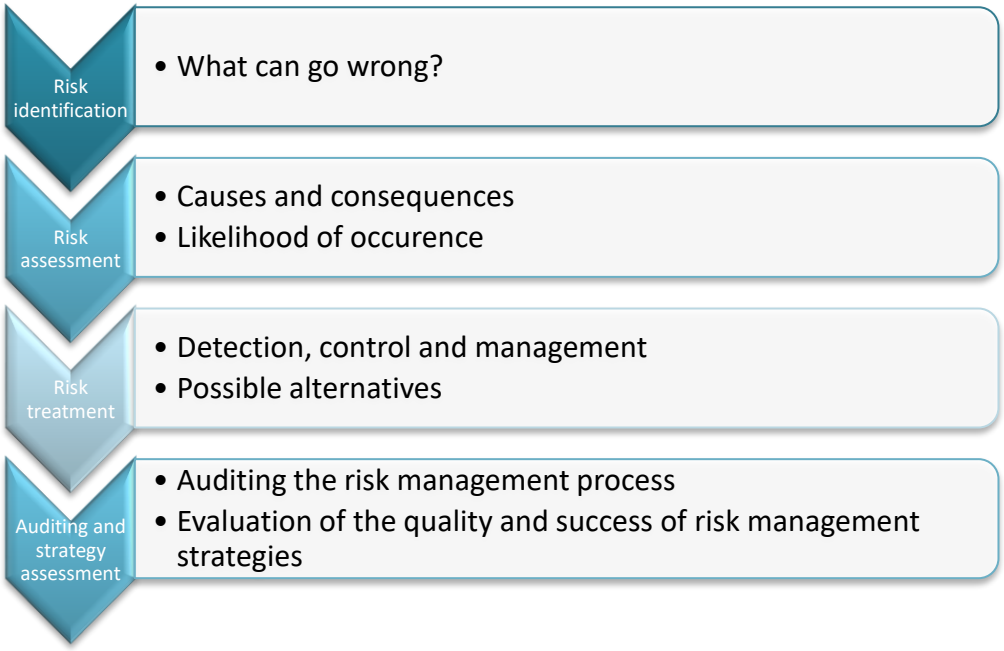

Figure 2 Stages in operational risk management synthesized from previous literature (Pinto et al. 2015, 15-16; Ilmonen et al. 2010, 31)

Risk identification can be a challenging task for a company. One way of identifying risks is to use historical information and comparative analysis especially if the company has previously documented occurred risks (Pinto et al. 2015, 17; Ilmonen et al. 2010, 105). In addition to documented information, knowledge of previously occurred risks can exist in the company in the form of tacit knowledge (Ilmonen et al. 2010, 116). Thus, interviewing employees of the company to transform such information into non-tacit might be a way to identify risks (Pinto et al. 2015, 18). By comparing historical information to the system under scrutiny can generate vital knowledge about the future risks for the system. Another way to identify risks is to examine existing lists of plausible risks. These types of risk registries are published, for instance, by federal agencies and professional and industry groups (Pinto et al. 2015, 19). In addition to these two methods, brainstorming with a multidisciplinary team and risk modelling (such as analytical, mathematical, physical and mental modelling) can be used to identify risks (Pinto et al. 2015, 20; Ilmonen et al. 2010, 106).

After the identification of plausible risks, the risk management process continues to risk assessment. The existing literature presents both quantitative and qualitative methods for this stage of the process (Fenz et al. 2014, 412). The purpose of risk assessment is to assess the likelihood of the risk, its causes and consequences (Pinto et al. 2015, 20;

Ilmonen et al. 2010, 106-109). Ilmonen et al. (2010, 95) suggest that the evaluation of the consequences ought to include the evaluation of the largest possible financial loss from the risk and how it has been calculated. Since doing business always involves a risk, aiming to eliminate all the risks is not the purpose of risk management (Ilmonen et al. 2010, 12). Thus, this stage helps the company to decide which risks are the most crucial to protect against. Cross referencing the likelihood of the risk with the severity of the consequences helps the company to prioritize and direct the available resources for where the risk is most probable and consequences most catastrophic for the company's operations (Pinto et al. 2015, 24). An example of such risk matrix has been drawn below in figure 3 utilizing a similar model from Ilmonen et al. (2010, 100) and Pinto et al. (2015, 24). The blue dots represent different risks identified in the first stage of the process and they have been located in the matrix based on the assessed likelihood and consequences. Using such matrix, the company can prioritize its available resources for mitigating risks that are closest to the top right corner.

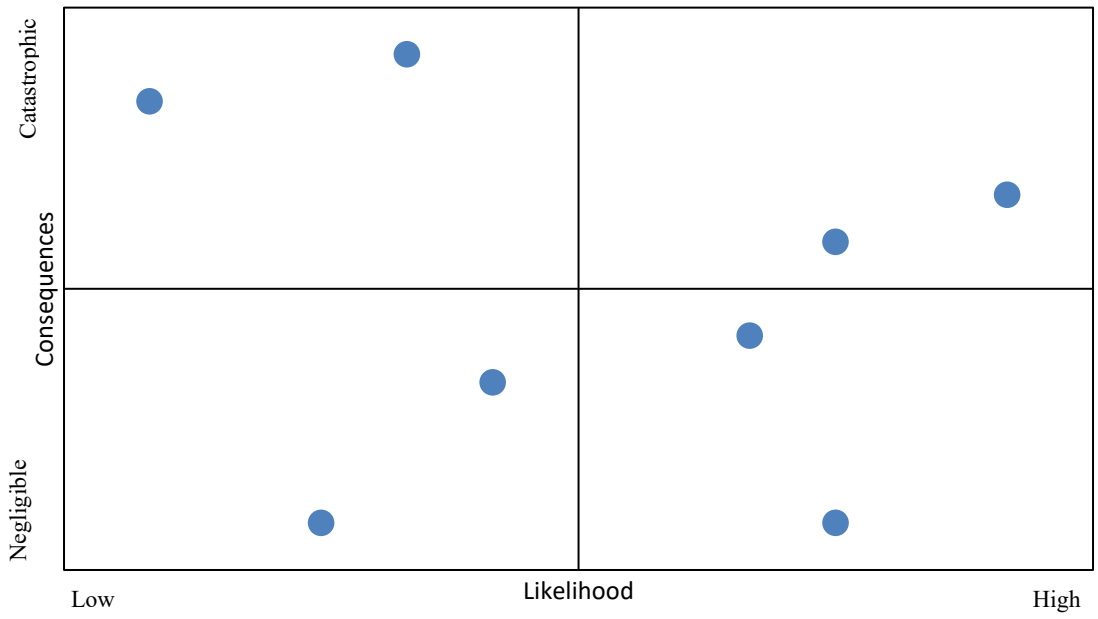

Figure 3 Risk assessment matrix (Ilmonen et al. 2010, 100; Pinto et al. 2015, 24)

After the careful assessment phase, a company can start planning its risk management strategy starting from the risks with highest priority. Pinto et al. (2015, 25) suggest that a team-based approach where experience and expertise is utilized for risk management strategy creation is often the most beneficial. Ilmonen et al. (2010, 124) suggest four

different approaches to treating risks. A company may either want to eliminate the risk completely, mitigate the risk, accept the risk or transfer the management of the risk for an external party. Figure 4 has been drawn from Ilmonen et al. (2010, 124) and represents the different risk management approaches and strategies that can be used with each approach. Eliminating the risk altogether is often not the optimal strategy even with high priority risks (Ilmonen 2010, 125). However, a company can choose to use an exit strategy and end the entire operation causing the risk if they do decide to eliminate the risk completely. Most companies, however, tend to mitigate or accept risks depending on the priority of the risk. The causal chains, identified in phase one, play an important role when risk mitigation strategies are planned. By identifying causalities, a company can assess which risk events in the causal chain can be managed to reduce their likelihood of occurrence (Pinto et al. 2015, 24-25 and Ilmonen et al. 2010, 97). Depending on the context, it might also be beneficial for the company to transfer the risk. Risks can be transferred for instance using deals (such as leasing contracts), financial instruments (such as derivatives) or insurances. Whilst the theoretical framework in this paper concentrates mainly on operational risk management solutions used to mitigate risks, it remains vital to recognize that other traditional mechanisms of risk management, such as derivatives and other financial instruments, are additionally often essential elements of companies' risk management strategies (Banks 2004, 3).

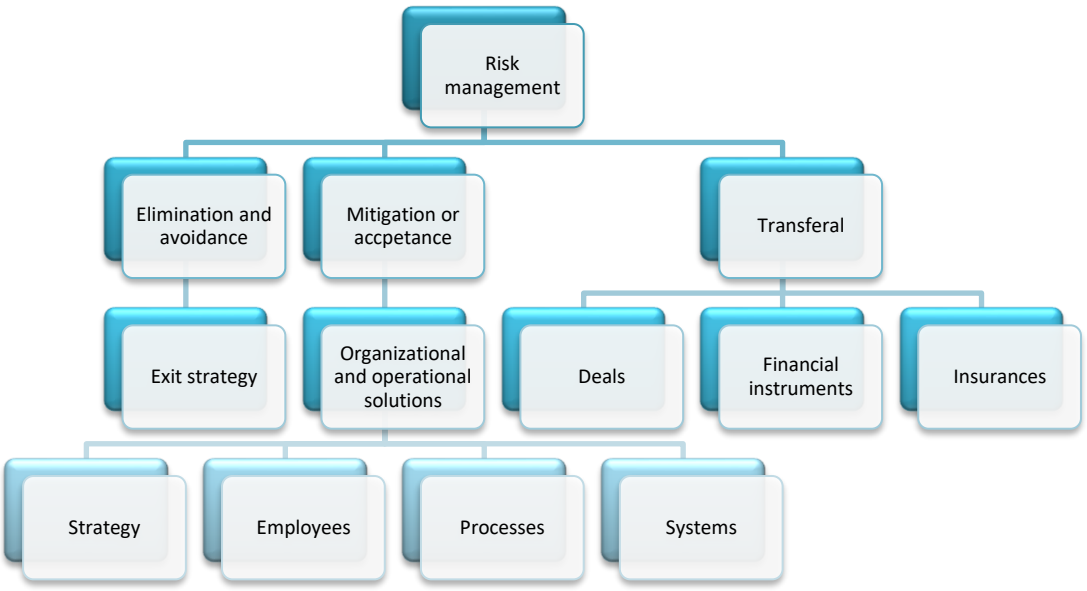

Figure 4 Risk management approaches

The last stage of operational risk management, auditing and strategy assessment, is additionally, an important part of the risk management process. With careful auditing of the risk management process, a company can later return to the analysis and utilize historical information when re-evaluating the risks and updating the risk management strategy. In addition, the company can then re-evaluate the quality of the risk management strategy and assess if there is a need for change. In addition, Pinto et al. (2015, 15) emphasize that different industries work in different contexts and thus, it is important that the context of the system is recognized and defined in order to improve operational risk management. Even though risk management strategies are highly context dependent, it might also be worthwhile to benchmark the risk management strategies in order to identify best practices form the field (Ilmonen et al. 2010, 197).

3.2 Cyber risk management

Cyber risk management is usually considered as a part of operational risk management (see, for example, Ilmonen et al. 2010, 71; Pinto et al. 2015, 11-12; Lam 2014, 244-245; Klapkiv & Klapkiv 2018, 242). Thus, theories in cyber risk management essentially often follow a similar process as discussed in the previous chapter (see figure 2) with a specific focus on cyber threats (see, for example, Ilmonen et al., 165-166; Refsdal et al. 2015, 36; Fenz et al. 2014, 415; Kendrick 2010). In addition, Limnéll et al. (2014, 165-212) have separated strategical, operational and technical levels for cybersecurity. According to this view, the identification and assessment of cyber risks would fall under the strategical level, management of the risks under the operational level, and practical actions to mitigate risks under the technical level. Hence, this chapter is aimed to deepen the focus of the theoretical framework introduced in chapter 3.1 by shedding light on the different stages of cyber risk management process. However, cybersecurity is a rather complex area of risk management and thus, full comprehension of the field requires often specific knowledge about information infrastructures. Thus, this chapter will mainly focus on the strategical and operational levels and will only touch the surface of the technical level of cyber security i.e. the practical methods and solutions used in cyber risk management.[4]

[4] For further reading about in-depth practical solutions for increasing cybersecurity see, for example, Rittinghouse and Hancock (2003), Kendrick (2010, 161-286), Kabanda et al. (2018, 271-273) and Limnéll et al. (2014).

The existing literature on cyber risk management uses different terminology often depending on the author and the specification of the publication. Although, the theoretical framework in this paper refers to cyber risk management, it has been constructed from existing publications that additionally refer, for instance, to IT risk management (see, for example, Ilmonen et al. 2010, 165-171; Kovácsné Mozsár & Michelberger 2018; Vincent et al. 2017), information security risk management (see, for example, Fenz et al. 2014; Chen et al. 2011; Saleh & Alfantookh, 2011) and cyber strategy (Limnéll et al. 2014). As mentioned earlier in chapter 1.1, cyber risks can be seen as risks caused by cyber threats. Thus, cyber risk management can be considered as the management of risks caused specifically by cyber threats (Refsdal et al. 2015, 33).

The failure of cyber risk management can have widespread consequences for the company's entire operation as cyber systems can have stakeholders and adversaries everywhere due to the nature of cyberspace (Refsdal et al. 2015, 34-35). Thus, whatever risk categorization method is used (see figure 1), it is important to note that cyber threats can be present in every category. Figure 5 below illustrates an example of how cybersecurity could be linked to every category of operational risks if the classification was done by the elements that constitute the system and its environment as Pinto et al. (2015) suggest. To understand cyber risks, it is essential for a company to understand the interaction of the system under scrutiny and cyber space (Refsdal et al. 2015, 37). Moreover, considering the links between the elements of the system and cybersecurity can also assist in recognizing goals and objectives, interrelationships among elements of a system and system boundaries from the perspective of cybersecurity (Ilmonen et al. 2010, 167). By understanding these links, companies can create cyber strategies that line with the goals and objectives of the company (Limnéll et al. 2014, 165).

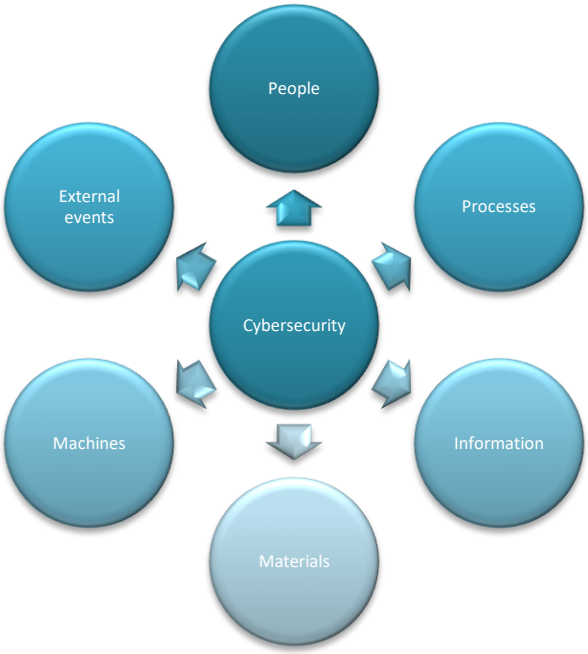

Figure 5 Operational risk classification (Pinto et al. 2015, 10) in relation to cybersecurity

The risks of cybersecurity violations can nowadays be considered as systemic risks for a company since the possible negative consequences of neglecting cybersecurity issues have increased significantly (Kaušpadienė et al. 2019, 980). The losses can include, for instance, direct economic losses, losses of intellectual capital, losses of confidential information, lost opportunities, damaged reputation, costs for customers and business partners, and additional costs of improving cyber security and recovering from the attack (Limnéll et al. 2014, 126-127). Systemic risk is often used in financial and economic paradigms referring to the collapse of the financial system. Here, however, the term refers more generally to the risk of a breakdown of the entire system, for instance a company's entire operation, as opposed to breakdowns in individual parts of the system (Ilin & Varga 2015, 245). The classification as systemic risk additionally indicates the importance of cybersecurity and cyber risk management. However, economic losses caused by cyber incidents are not universally similar to every actor or company in the world. Instead, the magnitude of the losses differs depending on the industry and competitiveness in the field (Limnéll et al. 2014, 126).

As mentioned earlier in the paper, the process of cyber risk management often follows roughly the same pattern as the stages of operational risk management introduced in chapter 3.1. Thus, the process of cyber risk management begins with identification of

plausible cyber risks. In order to identify cyber risks caused by malicious cyber threats, it is often beneficial to start with identifying possible threat sources (Refsdal et al. 2015, 35) and consider if there are some industry specific threats or threat sources (Ilmonen et al. 2010, 166). Different sources can include, for instance, nation states, terrorist groups, companies, criminals, hacktivists or other individual actors (Limnéll et al. 2014, 113). Due to the nature of cyber space, the number of possible threat sources can be extremely large and thus, complicate the identification of all possible threat sources (Refsdal et al. 2015, 35; Tawileh et al. 2007, 332). However, if or when a source of a malicious cyber threat is identified, the next step is to identify the motives, intentions, abilities, skills and resources of the source in order to examine how the source might be able to harm the company's operations and assets (Refsdal et al. 2015, 36, 38). Different motives can include, for instance, political or military power gains, aims for political change, aims to increase fear, aims to steal information, financial gains, or egoism (Limnéll et al. 2014, 113).

Identifying non-malicious cyber threats, on the other hand, is far more complicated as these risks are often caused by accidents and failures (Refsdal et al. 2015, 36). With these types of risks, a company can start with focusing on the company's assets (Refsdal et al. 2015, 36, 41) and processes (Limnéll et al. 2014, 170-171) and analysing their cyber vulnerability and how they might be harmed. Limnéll et al. (2014, 170-171) have identified some examples of assets and processes that can be vulnerable for cyber threats. These examples are illustrated in figure 6. After identifying these plausible incidents for these assets and processes, the company can consider what types of vulnerabilities can lead to such incidents (Refsdal et al. 2015, 42) and which threats and threat sources could arise from such vulnerabilities.

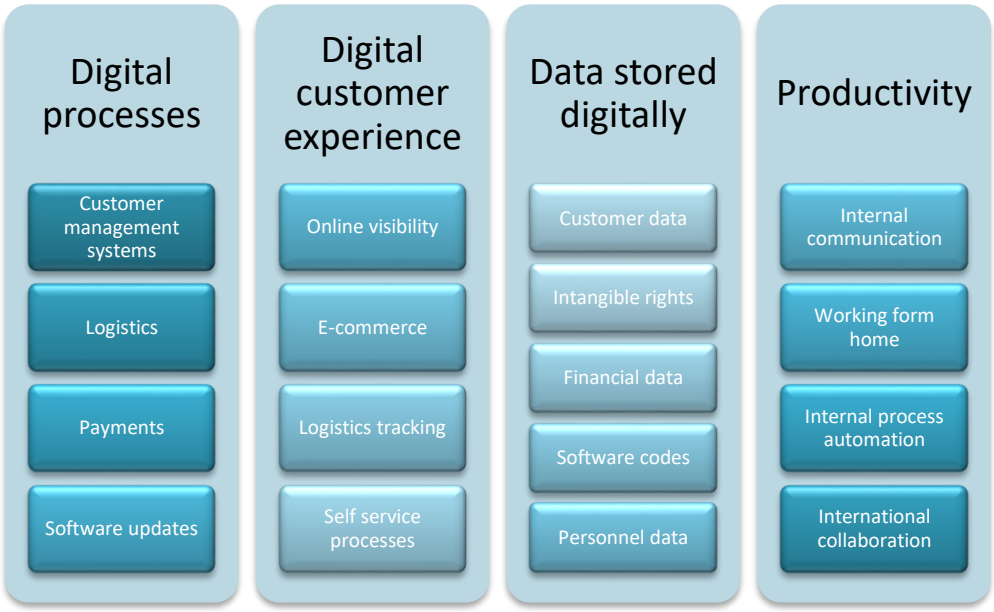

Figure 6 Cyber vulnerable processes and assets from Limnéll et al. (2014, 171)

Since the identification of malicious and non-malicious cyber threat sources and cyber threats can be quite challenging, companies might often need additional information about possible threat sources. Hence, as discussed in the previous chapter relating to operational risks in general, companies can utilize different information sources to facilitate the identification of malicious or non-malicious cyber threat sources, cyber threats and vulnerabilities. These information sources include, for instance, international standards, historical information, tacit knowledge, security testing, brainstorming, and existing reports of possible cyber threats by professional industry groups (Refsdal et al. 2015, 39-42).

As discussed in the previous chapter, after identification of different threats, the company needs to assess the risks' consequences and their likelihoods. Risk assessment, in terms of cybersecurity risk management, requires capturing the linkages between IT components and the company's other assets, values and operations in order to assess the consequences these risks carry (Kendrick 2010, 114). Assessing especially malicious cyber threats can be quite complicated compared to assessment of some other operational risks due to the difficulty of estimating the likelihood of malicious cyber threats (Refsdal et al. 2015, 43). However, existing lists from professional industry groups and security testing of vulnerabilities can help in the assessment of the likelihood of the risk and the severity of the consequences of both malicious and non-malicious cyber threats (Refsdal et al. 2015, 43). Additionally, analysing the capabilities, resources and motives of the

plausible attack sources in the identification phase can facilitate the estimation of likelihood of the risk with malicious cyber threats (Refsdal et al. 2015, 43). Moreover, it is often sufficient to estimate the relative likelihood against other threats instead of the real likelihood of the threat in order to detect the most severe risks (Ilmonen et al. 2010, 165).

Once the consequences and likelihoods of the cyber risks are evaluated a company can decide how to treat the identified cyber risks. Hence, risk management strategy depends on whether the risk needs to be eliminated, mitigated or transferred (Ilmonen et al. 2010, 166). In order to efficiently manage cyber risks, it is often beneficial to prioritize cyber risks that have the most severe consequences and are most likely to occur (Refsdal et al. 2015, 44-45; Ilmonen et al. 2010, 166; Mukhopadhyay et al. 2019; Limnéll et al. 2014, 175). In addition, the chosen risk management strategy often depends on whether the cyber risk is malicious, non-malicious or both. For instance, complete elimination of the risk is almost impossible if the cyber threat is malicious (Refsdal et al. 2015, 44; Kendrick 2010, 110). However, in order to mitigate cyber risks (especially non-malicious cyber risks), a company can, for instance, increase security awareness and training, implement technical barriers to reduce the likelihood of information leakages, and generally improve their processes and routines (Refsdal et al. 2015, 44).

When planning the cyber risk management strategy, it is important to consider the costs, the implications on performance, and the perspective of the end-user. Often the decision makers naturally evaluate the direct costs of risk mitigation strategies. However, especially with cyber risk management tools, the usability and performance might be affected and thus, the investments in cybersecurity can have unexpected negative consequences for the operations (Refsdal et al. 2015, 45). Brainstorming, questionnaires, interviews, existing lists and databases can help analysing the cost-effectiveness of the cybersecurity strategy (Kendrick 2010, 118-119).

Due to the nature of cyber space, there are often cyberthreats that cannot even be identified. Thus, the company needs to, additionally, evaluate the need for building cyber-resilience against unknown threats (Limnéll et al. 2014, 177). In addition to creating proactive risk management strategies, it is important to plan how the company can recover if these risks events cannot be prevented (Pinto et al. 2015, 24) and how the continuation of the business can be ensured (Limnéll et al. 2014, 225). Hence, it is important that the company has a strategy for handling risks that are already occurred as well as a business

continuity strategy. Refsdal et al. (2015, 35) emphasize, additionally, the importance of having an efficient communication strategy in case of an occurred cyber incident.

Monitoring and assessing the risk management strategies is crucial in cyber risk management due to the dynamic and continuously fast-changing environment. Due to this nature of cyber space, ideally the performance assessment of cyber risk management would be largely computerized in order to achieve effectiveness that the context requires (Refsdal et al. 2015, 46). Refsdal et al. (2015, 35) also suggest auditing and regularly updating all relevant information regarding cyber risk management during the entire process. This information could include, for instance, possible cyber threats, vulnerabilities and incidents, adversary profiles and company's strategies for cyber risk mitigation (Refsdal et al. 2015, 35) as well as data about the frequencies of cyberattacks (Refsdal et al. 2015, 46).

Lastly, even though the scope of this paper is to focus on cyber risks and cyber risk management, it is important to notice that a part of cyber strategy is to, additionally, consider the opportunities that digitalized processes create (Limnéll et al. 2014, 181-187). Even though cyber risks and their consequences should not be underestimated, it is important to recognize these opportunities and thus, find a balance of the cyber opportunity management and the cyber risk management (Limnéll et al. 2014, 223).

3.3 Cyber risk management challenges for SMEs

As mentioned earlier, operational risk management and cyber risk management ought to be contextualized to suit the industry specific environment. However, in addition to the industry specific context, SMEs usually operate in different conditions than larger organizations and thus, should apply operational risk management and cyber risk management processes to suit their goals and resources. Therefore, many cybersecurity strategies developed for larger organization are often not feasible for SMEs (Tawileh et al. 2007, 331). In order to, therefore, examine the research problem and questions posed earlier in chapter 1.2, it is important to deepen the understanding of the theoretical framework in the context of SMEs. Hence, this chapter aims to shed light on some of the challenges recognized in the previous literature that SMEs often face regarding cyber risk management.

For any sized company, it is important to optimize the available resources when creating a cybersecurity strategy (Limnéll et al. 2014, 226). Therefore, one of the most

crucial aspects that create challenges for SMEs' cybersecurity, is the limited resources these companies often possess (Kaušpadienė et al. 2019, 979; Kabanda et al. 2018, 269; Tawileh et al. 2007, 332; Kurpjuhn 2015, 5). This resource scarcity in SMEs often includes, for instance, limitations in human resources, limited knowledge and awareness about the company risks and especially cyber threats, deficiencies in processes, and limitations in monetary and technical resources (Boustras & Guldenmund 2017, 6; Tawileh et al. 2007, 332-333; Bada & Nurse 2019, 394). Thus, SMEs operational risk management and cyber risk management processes are naturally constrained and thus, should be implemented using the available resources (Boustras & Guldenmund 2017, 10).

One of the most common problems of efficient cybersecurity is a lack of IT governance (Julisch 2013, 2210). Hence, partly due to the limitations in human resources, especially SMEs often have large gaps in IT governance since SMEs often do not have a dedicated IT management department (Kabanda et al. 2018, 269-270). In fact, Ilmonen et al. (2010, 165) mention that very often company's overall IT governance has been neglected and instead, cybersecurity is depending on individual departments. This lack of undefined or unclear processes and responsibilities often creates vulnerabilities for the system (Julisch 2013, 2209-2211) since cybersecurity issues may be presumed as someone else's responsibilities and therefore, decisions regarding cybersecurity might be made in an ad-hoc manner or not at all (Julisch 2013, 2210). Hence, in order to identify cyber risks, it is often mandatory to first implement some basic IT governance operations (Ilmonen et al. 2010, 165).

In addition to implementing basic IT governance operations, it is crucial that cyber risk management frameworks directed for SMEs are compact (Kaušpadienė et al. 2019, 979) in order for SMEs to feasibly develop and enhance their cyber risk management processes. The importance of these compact guidelines is emphasized especially if cyber risk management is not outsourced but instead, for instance, left for the manager or owner's responsibility. In order to achieve this research's objective of adding theoretical contribution to the field, chapter 3.4 has been created iteratively with the study's results and will synthesize some of the main considerations of cybersecurity strategies in the context of SMEs. In addition, the strategical and operational suggestions for improving SMEs cybersecurity have been introduced in chapter 5.3.

In addition to limited human resources, another challenge for SMEs tends to rise from lack of awareness and expertise (Bada & Nurse 2019, 394; Tawileh et al. 2007, 332), limited knowledge about the company risks (Boustras & Guldenmund 2017, 6), and the

lack of management support and attitudes towards cyber risk management (Kabanda et al. 2018, 274-275; Bada & Nurse 2019, 397). In SMEs, risk identification and risk assessment are often left for the manager or owner of the business (Boustras & Guldenmund 2017, 10) and cyber threats are often not taken seriously (Kabanda et al. 2018, 270). In addition, Julisch (2013, 2207) has found that decision-makers often rely heavily on intuition and own experience as opposed to statistics when assessing the probability and impact of a cyber threat due to cognitive biases. Therefore, there is a chance that threats with statistically high likelihood and severe consequences might not be assessed and managed accordingly. This in turn, might also affect the level of preparedness against cyber threats in general. Moreover, Julisch (2013, 2208-2209) has found that companies tend to rely heavily on knowledge within products such as virus scanners as opposed to building intelligent risk management strategies. Due to the dynamic nature of cyberspace and cyber threats, this over-reliance can often affect negatively the level of cybersecurity in a company.

Kurpjuhn (2015, 5) and Kabanda et al. (2018, 270), additionally, refer to a common misbelief among SMEs that cyber criminals would have no motivations and incentives to target small businesses since there are so many large corporations that they can target instead. These misconceptions are additionally discussed in an article by Paulsen (2016, 92) as she mentions that according to a survey by KMPG “half of small businesses thought there was little risk of being the target of an attack” even though previous research show different results as discussed in chapter one.

In his article, Nam (2019) examined the perceptions towards cyber security and cyber threats. He discovered that political liberalism and social trust tend to decrease the level of perceived cyber threats and increase the level of perceived cyber-resilience (2019, 1). In contrast, awareness and previous experiences of cyber threats tend to increase the level of perceived threats and decreased the level of perceived cyber-resilience (Nam 2019, 1). All in all, based on Nam’s research (2019), it seems that different attributes affect individuals’ perceptions and attitudes towards cyber threats and cyber-resilience. Hence, it is possible that the actual level of preparedness against cyber threats might vary partly due to attitudes around the issue which in turn might be affected by other attributes such as awareness, experiences, political ideology and the level of trust.

The lack of awareness and management support can also affect the cybersecurity culture in the company. A good cybersecurity behaviour by the employees of the company is, thus, another concern for SMEs (Bada & Nurse 2019, 397) and as mentioned

earlier in the paper some studies show that only 9% of SMEs have cybersecurity cultures (Kaušpadienė et al. 2019, 980). Yet, Bada and Nurse (2019, 397) suggest that creating a security culture is crucial since developing such culture and, therefore, increasing employee knowledge can increase the company's overall security level significantly (Bada & Nurse 2019, 399).

Lastly, one of the most crucial challenges for SMEs are the limited financial and technical resources as mentioned earlier (Boustras & Guldenmund 2017, 6). Cyber risk management can be expensive, time consuming and require investments to increase knowledge and awareness (Limnéll et al. 2014, 225; Tawileh et al. 2007, 332). Thus, the phase of risk assessment becomes especially important for SMEs due to this financial resource scarcity. Hence, it is crucial to evaluate which risks have the highest likelihood to occur and which risks might have the most devastating consequences for the company (Boustras & Guldenmund 2017, 9-24). When working with limited resources, the company can, thus, prioritize the most likely and severe risks after a careful assessment and direct resources for risk mitigation plans towards these risks.

In conclusion, based on previous research, there are quite a few different constraints that can affect SMEs cybersecurity preparedness. These constraints are mostly related to resource scarcity and limited knowledge and awareness of cybersecurity issues. The next chapter aims to draw a synthesis of the previous chapters of operational and cyber risk management considering the SME perspective and the challenges related to SMEs cyber risk management.

3.4 Theoretical synthesis: cyber risk management in SMEs

The theoretical framework presented above in chapters 3.1, 3.2 and 3.3 has been drawn from publications that examine operational risk management, cyber risk management and challenges SMEs struggle with concerning cyber risk management. Hence, this chapter aims to draw a theoretical synthesis from the previous chapters focusing specifically on the context of SMEs and the constraints these companies operate under. In order to draw such a synthesis and apply the model of cyber risk management to the context of SMEs, this chapter has been created iteratively using both existing theories and the empirical findings from this research. This iterative process has been discussed further in chapter four.

As mentioned previously, SMEs operate in different contexts and in order to create optimal cyber risk management strategies, they need to be designed under these context specific requirements. Thus, optimal SME's (cyber) risk management strategy depends on the goals and objectives of the company, the industry the company operates in and its crucial assets, the resources the company obtains and other internal and external aspects. As previous literature indicates, there are often constraints and challenges that SMEs encounter considering cyber risk management strategies mostly due to resource constraints and awareness. This chapter aims to illustrate the process of cyber risk management for SMEs, the challenges these companies might face and possible solutions to tackle these obstacles.

Table 1 below illustrates the process of cyber risk management including contextual requirements and constraints SMEs are often forced to operate under and possible solutions to tackle these constraints. It has been synthesized from different publications that have been referred to in the previous chapters of this paper, as well as from the empirical findings emerged from this research. The top row of the table describes the importance of defining the framework the company operates under. This overall framework shapes the cyber risk management of the company. For instance, companies operating in different industries might have different needs for cyber security due to some industry specific aspects. For instance, a company working in construction might face very different cyber threats than a company working in banking and finance or gaming industry. The framework umbrella, additionally, includes the (internal and external) environment such as political, economic, social, technological and legislative environment, as well as, stakeholders of the company, size of the company, resources of the company etc. All in all, there are many aspects that affect the company's entire operation and thus, also, the optimal cyber risk management.

Table 1 Cyber risk management and challenges for SMEs

FRAMEWORK (industry, internal and external environment, stakeholders, size, resources etc.)			
	Step of the process	**Challenges for SMEs**	**Possible facilitators and practicalities**
Strat...	Recognizing goals, objectives,	• Failure to understand the interdependence	• Increasing awareness, for instance, from online

	critical assets and resources	between cyber space and critical assets and resources • Failure to consider data & processes as critical assets	sources (videos, blogs, articles etc. from professionals and other industry groups) • Checking if data and processes are or should be included in the list of most critical assets
	Cyber risk identification	• Lack of IT-governance (unclear responsibilities) • Limited knowledge, awareness and expertise • Limited human resources • Time constraints	• Assigning clear responsibilities • Using existing lists and registries to identify threats • Using external consulting services • Assessing cyber vulnerabilities of the critical assets and processes (with the help of existing lists)
	Cyber risk assessment (causes, likelihoods and consequences)	• Limited knowledge, awareness and expertise • Limited human resources • Time constraints	• Using existing lists and registries to analyse and evaluate risks • Only evaluating *relative* likelihoods and consequences against other threats • Using external consulting services
Operational	Cyber risk treatment strategy	• Limited knowledge and expertise • Limited human resources	• Prioritizing risk treatment on risks with highest likelihoods and

		• Lack of technical resources • Monetary costs (seen as low ROI) • Lack of management support and attitudes • Lack of cyber security culture	most devastating consequences • Transferring the risk → insurances • Using external consulting • Increasing staff awareness • Repairing solutions (continuation strategy) • Detective solutions (antivirus programs &firewalls)
	Auditing and re-assessment	• Limited knowledge, awareness and expertise • Time constraints • Monetary costs	• Understand the importance of monitoring and reviewing due to changing environment • Monitoring helps the ongoing threat identification

As shown in table 1 above, lack of awareness and knowledge, attitudes towards cyber risk management and cyber risks, as well as resource scarcity seem to create the most significant challenges for SMEs cyber risk management. Often same challenges appear in different stages of the risk management process and especially lack of awareness and attitudes might threaten the entire cyber risk management ever being considered as a part of an SME's strategy if in an early stage the management level fails to understand the interdependence between cyber space and the company's critical assets and resources. However, the last column of the table shows some practical advice on how these challenges might be tackled to facilitate SMEs' cyber risk management. The opportunities in the last column will be discussed more thoroughly in the analysis of the results in chapter 5.3.

The theories from previous literature presented in this chapter have worked as a theoretical framework for this research. Therefore, the theories from previous literature presented here, have additionally assisted in the analysis of the empirical findings and consequently, finding answers to the research problem and questions posed earlier in chapter 1.2. Thus, these theories will be returned to later in the paper in chapter five where results of the empirical findings are introduced more thoroughly. Due to the objectives of the study, the aim is to strengthen the models from previous literature with the empirical findings and apply them to better suit the context of SMEs. Moreover, from the more practical standpoint, the aim is to find suggestions on how Nordic SMEs could improve their cyber risk management strategies regardless of the identified challenges these companies can encounter.

4 METHODOLOGY

This chapter aims to explain how the research process has been completed and the rationale for why this strategy has been used to examine the research problem introduced in chapter 1.2. Chapter 4.1 begins by describing the philosophical assumptions that form the paradigm and thus, the framework for the entire research. The philosophical assumptions, additionally, construct the basis of the research strategy. Therefore, chapter 4.2 continues by presenting the above-mentioned research approach and strategy used to facilitate finding answers to research problem and questions. Chapters 4.3 and 4.4 will go further into the methods used to gather the empirical data and to analyse it. Lastly, chapter 4.5 aims to address the quality of the research by assessing the trustworthiness and authenticity of the research.

4.1 Underlying philosophical assumptions

This chapter aims to describe the philosophical assumptions that form the broader framework for the entire research. These ontological and epistemological assumptions construct the paradigm under which the research has been conducted. Ontological assumptions in this research refer to the assumptions about the nature of social phenomena around cybersecurity and the management of cybersecurity, whereas epistemological assumptions refer to the assumptions about the how these social phenomena should be studied and what is regarded as acceptable knowledge (Bryman 2012, 6, 27, 32; D O'Gorman & MacIntosh 2014, 55, 58-59).

Practical cyber risk management tools are often methods that we can sense concretely such as IT-security education for employees or installed antivirus programs. Thus, ontologically one could think objectively that only phenomena that can be sensed, exists in the context of this research. However, making such ontological assumptions that deny the existence of intangible or abstract and subjective phenomena, might limit the possible interpretations from the empirical data and hence, this objective ontological assumption is not made here. Instead, it is assumed that social phenomena, such as risk cultures in companies, are socially constructed and developed. Hence, it is additionally assumed that the social phenomena are not external to the people but instead, people are in the centre of this reality construction. This view is especially present in research question 2 where the research focuses on the current state of cyber security in SMEs and why it seems that

most SMEs have not prepared against cyber security threats. Even previous research emphasizes the role of people regarding the state of cyber security and thus, in this research the ontological assumptions are more leaning towards subjective constructionism rather than objectivism.

As mentioned earlier, the epistemological considerations refer to the assumptions of how these subjective and socially constructed phenomena around cyber security can be studied and what can be regarded as acceptable knowledge. First, as mentioned previously, the source of the reality is leaned towards a subjective perception of the world and reality since people are in the centre role of this reality construction. Hence, in this research, the epistemological assumptions lean towards interpretivist paradigm (D O'Gorman & MacIntosh 2014, 64-65). Since interpretivism shifts the focus towards understanding than just measuring (D O'Gorman & MacIntosh 2014, 65) the phenomenon of cybersecurity in Nordic SMEs, it is assumed that acceptable knowledge could be obtained by conducting semi-structured interviews with experts in the field who would be relevant considering the objective of the research and the research problem.

Therefore, the knowledge obtained from the research reflects the interviewees' and interviewer's perceptions of the reality around cybersecurity. Additionally, the assumption is that this knowledge can be generalized to a certain degree considering the contextual specificities. However, it is important to keep in mind that the results found in the research are derived from a certain context and thus, the knowledge obtained from the results is not meant to be generalized universally in a wider sense.

It could be argued that it would be difficult, if not impossible, to conduct a perfectly objective research in the context of the research problem and questions. Especially since based on previous literature, it seems that attitudes and cognitive biases affect the level of cybersecurity in SMEs. Hence, instead of taking a positivist standpoint, here it is assumed that the knowledge is dependent on the interpretation of the reality and thus, people (in this case for example the interviewees and the researcher) have constructed their interpretations of the reality based on their experiences and knowledge. Since the point is not to search results that would be universally generalized, the interpretations and subjectivity are considered rather as an asset than a limitation for this research since it enables to focus on understanding the phenomenon of preparedness against cyber threats rather than just measuring it (D O'Gorman & MacIntosh 2014, 65).

4.2 Research approach and strategy

The research problem in chapter 1.2 was formulated to examine the level of preparedness against cyberattacks in Nordic SMEs and to discover whether there would be room for improvements regarding that level of preparedness. Therefore, this research methodology follows a qualitative approach since it allows to gain more in-depth knowledge and understanding (D O'Gorman & MacIntosh 2014, 66) about the state of cybersecurity, risk strategies and improvement possibilities of cybersecurity practices in SMEs. Furthermore, since a qualitative approach is better suited for examining the research phenomenon through the eyes of the research participants (Bryman 2012, 412), it has enabled the gathering of more in-depth data by going deeper into the mindsets of the research participants and asking follow-up questions whenever necessary. In addition, the ontological and epistemological assumptions, mentioned in the previous subchapter, direct the research additionally to qualitative methodological strategy (D O'Gorman & MacIntosh 2014, 59). Lastly, since neither the research problem, nor the research questions necessarily required measuring or quantification of data related to cybersecurity, qualitative approach offered a better approach for finding answers to the research problem and questions. Therefore, a qualitative approach has been selected to best suit the research context and the philosophical assumptions discussed in the previous subchapter.

As mentioned previously in chapter three, the process of this research and more specifically, the relationship between theory and research has been iterative. Hence, the theoretical background and empirical research have been constructed simultaneously, combining both inductive and deductive methods (Eriksson & Kovalainen 2016, 23-24). In order to find answers to the research problem and questions posed in chapter 1.2, it is crucial that the researcher is reasonably familiar with the phenomena of cyberspace and cybersecurity. Hence, the process was started by building knowledge on cybersecurity by talking with acquaintances who are working in the field or otherwise familiar with the field. In addition, in the beginning of the process news articles, online sources and academic publications were read in order to find relevant information and to familiarize with the subject. This initial learning process, additionally, helped in finding of plausible knowledge gaps in existing research and formulating a research problem that would, in the best-case scenario, add both academic and practical contribution to the field. Hence,

during this early stage of familiarization to the subject, the research questions were edited and formulated to better complement the existing knowledge.

The gathering of the research data started quite early on in the process, once the understanding about the field of cybersecurity was sufficient enough. The process of data gathering started early so that contextual understanding of the field of cybersecurity in Nordic SMEs could be increased. Since the focus of the research shifted from examining the current state of cybersecurity in Nordic SMEs to examining why the level of cybersecurity among SMEs is generally rather low, the theoretical framework was additionally constructed and concentrated simultaneously more towards the modified research questions. Hence, chapters 3.1-3.3 were developed simultaneously while the gathering of empirical data was already in progress. In addition, the synthesis of the theoretical framework in chapter 3.4 where the existing theories were synthesised and adapted to suit the context of SMEs was created and developed iteratively as more results were gathered and analysed.

Therefore, chapter 3 and especially chapters 3.4 and 5 (where the results from the empirical data are presented and discussed) have been developed from the intercommunication between the simultaneous accumulation of theoretical framework and empirical findings. Eventually, this research process followed rather similar steps as Bryman (2012, 384) has described in the context of qualitative research. Figure 7 demonstrates these steps introduced by Bryman (2012, 384) in the context of this particular research process.

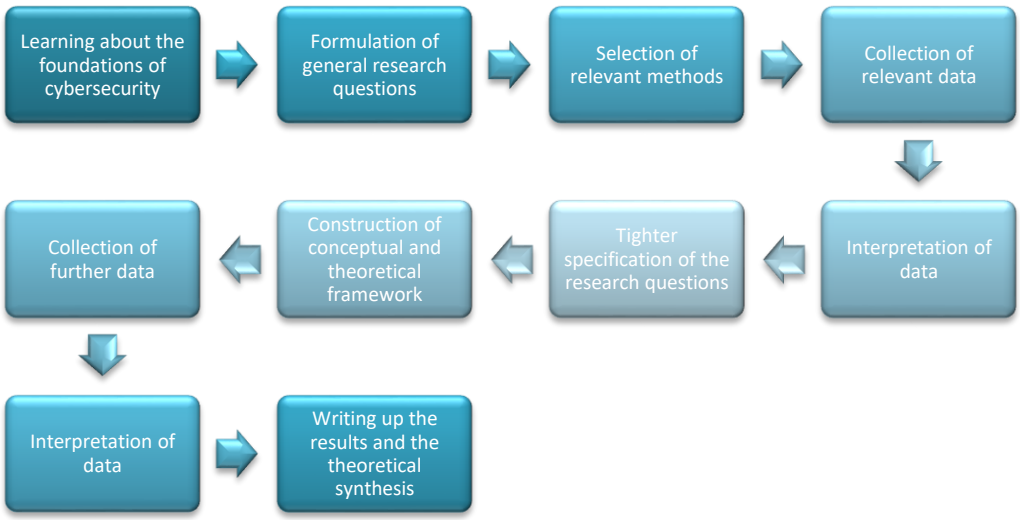

Figure 7 Outline of the main steps of the research (edited from Bryman 2012, 384)

Lastly, the research design is analysed based on the nature of the research problem and questions. Since the research problem is concerned with examining the state of cybersecurity in Nordic SMEs and more specifically to find explanations to why the level of cybersecurity is generally low in Nordic SMEs, the research design could be considered mainly explanatory (D O'Gorman & MacIntosh 2014, 82). However, the other part of the research problem has a more normative angle and aims to increase knowledge on how these SMEs could increase their level of cybersecurity. The more normative and practical answers to this second part of the research problem were constructed mainly by applying existing theories in the context of SMEs based on the empirical findings. Thus, this part of the research design could be regarded as a bit more exploratory as the existing research for this particular context was more limited (D O'Gorman & MacIntosh 2014, 82).

4.3 Data collection and interviewee selection

The data of the research has been collected by conducting semi-structured interviews with industry experts and representatives who work with cyber security issues or are responsible for IT-security in a company. Since the nature of cyber security is quite complex and based on previous literature there is a possibility that companies, especially SMEs, will not always even detect cyberattacks, the inclusion of industry experts was essential in order to investigate the research problem and find answers to the research questions. After considering different data collection methods, conducting semi-structured interviews appeared to suit best for the purpose and objective of the research: to find out why the preparedness in Nordic SMEs varies and to seek solutions for improving that level of preparedness. Therefore, this method was chosen because the aim was to research the topic from the perspective of the interviewees (Cassel & Symon 2004, 32).

If the research questions were considered separately, there would also be other relevant alternatives to collect the data. To investigate why most Nordic SMEs do not prepare for cyber risks (research question 2) could very well also be studied by using the methods of ethnography, participant observation, or conducting interviews from SMEs' representatives. However, by only using one these methods the two additional questions of what kind of cyber security risks these companies face and what could be done to

improve the preparedness in SMEs would most likely be left unanswered in comparison with gathering data by interviewing industry experts. In addition, conducting interviews was the most feasible method for data collection. The data collection method of ethnography or focus groups, for instance, would most likely have required absence from work as well as much more in depth knowledge about cyber security as a phenomenon compared to interviewing experts of the field.

In a qualitative research, interviews are typically unstructured or semi-structured (Bryman 2012, 470; Cassel & Symon, 32). In the context of this research, the semi-structured interviews supported more the objective of the study since the interviewees are experts in the field and have such an extensive knowledge about the subject. Thus, using a semi-structured interview helped in shifting the discussion towards relevant issues from the point of view of this research if the discussion shifted too far from the topic. In addition, formulating the interview guide helped in the process of formulating relevant questions that would support and complement the knowledge already gathered from previous literature.

However, the interviews were meant to be flexible and give the interviewees an opportunity to bring up issues that might have otherwise not come up. Consequently, the interview guide was merely a supporting tool and was in some cases tailored according to the interviewee's background. In addition, in most cases, the interviews did not follow the exact schedule presented in the interview guide. The flexibility additionally allowed the interviews to generate rich and detailed answers (Bryman 2012, 470) which was one of the main points of conducting the study as a qualitative research. The interview guide is attached to the end of this paper (appendix 1).

The research participants i.e. interviewees have been selected using a method of purposive sampling. Purposive sampling is a fundamental selection method in qualitative research approach and highlights the research questions as the basis for selecting the participants (Bryman 2012, p. 428). As mentioned earlier in this chapter, conducting interviews from industry experts facilitated in finding answers to all of the research questions posed earlier in chapter 1.2. In addition, due to the research scope being limited to SMEs operating in the Nordic countries, it is important that the data is collected from experts who are familiar with the state of cybersecurity specifically in this context. In order to achieve results in a wider perspective about the state of cyber security in SMEs operating in the Nordic countries, the method of purposive sampling was, therefore, used to choose the research participants. As opposed to interviewing a few SME CEOs, for

instance, interviewing these industry experts gives a broader viewpoint to the state of cyber security and the phenomenon in general, thus, adding the trustworthiness and authenticity of the research.

Therefore, the data has been collected conducting semi-structured interviews from six different industry experts. For the sake of protecting the interviewees' request for anonymity, their backgrounds are not described in detail in this paper. However, all six interviewees had a long experience working in the field of cyber security issues and had extensive knowledge about the phenomenon as a whole in the Nordic and Baltic countries due to their careers. Their backgrounds of working in the field enabled them to discuss for instance about the different cyber threats, the state of cyber security in the Nordic countries and different methods of protecting companies from these threats. Most of the interviewees had focused on larger enterprises during their career but were still additionally familiar with the phenomenon in the context of SMEs.

Out of the six interviews, three were conducted as telephone meetings for feasibility purposes. The interviewees' tight schedules and physical locations made telephone meetings the best choice of method. Two of the interviews were conducted face-to-face and one was conducted as a video conference which allowed the researcher to additionally study the expressions and overall ambiance of the interview situation. The interviews lasted from 40 minutes to 1.5 hours. All six interviews were recorded and transcribed to facilitate the analysis of the results later on in the process.

As mentioned earlier in this chapter, an alternative method of conducting interviews from SME representatives would have enriched the data for research question 2 of why Nordic SMEs do not generally prepare against cyber threats. In addition, it would have strengthened the trustworthiness related to the assumption made in the research that most SMEs in fact do not prepare for these threats. Hence, to increase the trustworthiness and strengthen the assumption made based on previous literature and industry experts' interview results, a structured interview in the form of a questionnaire was developed. This questionnaire was directed towards SME representatives in order to gain further data from entrepreneurs in addition to the data gathered from the industry experts in the form of semi-structured interviews. An incentive for responding to the questionnaire was created in the form of a list of tips for improving SMEs cyber security practices (see appendix 2) and the questionnaire was marketed in different social media channels. Unfortunately, however, the number of respondents from SMEs representatives was minimal (in total three responses from SME's representatives). Hence, for the sake of

protecting the trustworthiness and authenticity of the study and avoiding skewed or biased results, these results were left out of the study's results and analysis.

4.4 Data analysis

As mentioned in the previous subchapter, the interviews were recorded and transcribed in order to facilitate the data analysis and thus, reporting the results. Regarding the state of cyber security preparedness among Nordic SMEs, the aim was to see whether the reasons for differences in the levels of preparedness from the empirical findings supported the reasons gathered from existing literature. The other side of the research problem was to study whether there are room for improvements in cyber security practices of Nordic SMEs. Hence, the aim was to apply the existing theories in the context of SMEs and thus, create contribution both theoretically as well as practically. According to Eriksson & Kovalainen (2016, 141) systematic coding is a suitable method for data analysis when the research is "grounded in existing theory and attempts to improve the theory, or to test it". Hence, the data was primarily analysed by using a method of coding to support the aim of the research.

Even though the underlying philosophical assumptions acknowledge the presence of subjectivism and interpretation, by using the method of coding, the data of the research could be analysed as systematically as possible in order to give reasoning for what has been done and how the conclusions in chapter five have been developed (Eriksson & Kovalainen 2016, 203). Hence, out of different data analysis methods, coding suited the best for this research to organize and analyse the data gathered from the interviews systematically and in order to support the existing literature and possibly filling the gaps found from the existing literature regarding the context of SMEs.

First, the transcripts were read a few times and notes about significant observations were written down related to the research problem and questions without thinking about the codes or themes much further. Therefore, it could be argued that the process followed the steps of open coding since these first "codes" arose as open notes from the data (Cassel & Symon 2004, 266). However, as a part of the iterative process, some preliminary interpretations were already made based on the interview data before the actual coding analysis. These preliminary interpretations were done in order to sharpen and edit the research questions and the focus of the research, as well as to facilitate the process of finding more relevant publications to use as theoretical framework.

Next, titles for codes that would best describe each significant observation were written down. Hence, continuing the data classification process in the steps of open coding (Eriksson & Kovalainen 2016, 2014; Cassel & Symon 2004, 266). The codes were also reviewed and edited a few times in the process. After open coding, the process continued on to axial coding. This stage was aimed to examine the different codes can be linked together to create explanatory categories whilst bearing in mind the research problem and questions (Eriksson & Kovalainen 2016, 2014). Finally, the last step of selective coding, was aimed to find plausible interlinkages between the categories and more general theoretical issues that might have either already come up in the theoretical framework or presented new theoretical suggestions (Eriksson & Kovalainen 2016, 2014). These steps in the coding process, in the end, assisted in the process of writing down both the theoretical synthesis in chapter 3.4 and the results in chapter five as a part of the iterative process.

4.5 Research evaluation: trustworthiness, authenticity and ethics

The quality of the research has been assessed using the two primary assessment criteria for qualitative research by Guba and Lincoln (Bryman 2012, 390): trustworthiness and authenticity. According to Guba and Lincoln (1985, 289-331), trustworthiness includes four criteria: credibility, transferability, dependability and confirmability. Furthermore, the authors have suggested additional five criteria to assess authenticity: fairness, ontological authenticity, educative authenticity, catalytic authenticity and tactical authenticity (Bryman 2012, 393). Thus, these four criteria evaluating trustworthiness and the four criteria evaluating authenticity are discussed further individually in this chapter to address the quality of this research. In addition, ethical principles used in this research have been introduced in the end of this chapter.

In order to ensure the credibility of the research, a technique of respondent validation was used. Hence, the findings of the research were provided for the research participants for confirmation that I, as the researcher, have correctly understood the social world under research (Bryman 2012, 390; Cuba & Lincoln 1985, 314). According to Lincoln and Cuba (1985, 314), member checks (i.e. respondent validation) “is the most crucial technique for establishing credibility”. By following this technique, the interviewees were given an opportunity to correct errors of fact or interpretation and confirm the adequacy of the data. In addition, to increase the credibility, the research has been conducted using methods of

good practice and this final paper will be made publicly available. Moreover, a method of triangulation was meant to be used in order to increase credibility of the research by using more than one source of data (Bryman 2012, 392; Cuba & Lincoln 1985, 305) i.e. gathering data in the form of structured interviews from SME representatives. Unfortunately, however, the amount of data was not sufficient to be used in the research. However, in order to address credibility, multiple sources and theories were studied and used related to cyber security in addition to gathering the empirical data, which could also be considered as a form of triangulation (Cuba & Lincoln 1985, 305) thus, adding the credibility of the research.

Transferability has partly been addressed briefly already earlier in the paper. Since, the objective of the study is not to generate universally generalizable information, it is a presumption that the results of the study are not meant to be transferrable. Thus, the research context is stated already in the first chapter of the paper. However, even with clearly defined context, it is important to note that due to the dynamic environment of cyberspace, it is very likely that results obtained in this research might evolve rapidly. Therefore, even though the context has been narrowed to SMEs operating in the Nordic countries, it cannot be assumed that all the results of the study would hold in a similar context at another time point, for instance. Additionally, even though the study is not limited to concern a certain industry, it has been mentioned in chapter five, that different industries can face different cyber threats. Hence, the reader ought to be careful when making judgements about the transferability of the results of the research due to the dynamic environment of cybersecurity and its contextual dependencies.

Dependability, on the other hand, has been assured by following a systematic auditing process (Bryman 2012, 392). All notes, transcripts, recordings and other documented material has been saved in an accessible manner and kept during the entire research process. In addition, the actual writing of the paper started early on in the process in order to better follow the different phases of the research process and kept a learning journal about the progression of the process. The purpose of the learning journal was initially to help progress in the research process, but also for the thesis supervisors to notify if something had been missed or the direction of the research had needed to be changed. This in turn has affected positively on the dependability of the research.

Finally, regarding trustworthiness, confirmability has been addressed by acknowledging in chapter 4.1 that the study cannot be fully objective, and interpretations have an impact on the research analysis due to the underlying philosophical assumptions.

However, the research process including the interviews and the data analysis has been conducted without letting personal values or theoretical inclinations affect the research process or its outcomes (Bryman 2012, 392-393). The iterative process has, additionally, facilitated the assurance of confirmability in a sense that the interviews and data gathering started when the existing theories or cybersecurity practices in SMEs had not yet been extensively studied. However, it can be assumed that subjectivity is present, and the results have been gathered and conclusions have been made through the researcher's own lens even while aiming towards objectivity.

In addition to trustworthiness, it is important to evaluate the authenticity of the qualitative research. To evaluate the authenticity, the five criteria mentioned above, have been used: fairness, ontological authenticity, educative authenticity, catalytic authenticity, and tactical authenticity (Bryman 2012, 393). Fairness has been ensured by selecting different expert interviewees with different backgrounds and experiences, thus, representing different viewpoints of the phenomenon (Bryman 2012, 393). Ontological and educative authenticity, on the other hand, thrive for members of the research to grasp a better understanding of the social milieu and perspectives of other members (Bryman 2012, 393). These two criteria have been ensured by attempting to generate valid information for SMEs operating in the Nordic countries about the state of preparedness against cybersecurity threats and what could be done to increase the level of cybersecurity in SMEs. Finally, catalytic and tactical authenticity ensure that the researcher is acting as a motivator for members of the research to engage in action to change their circumstances and helped the members to take the necessary steps to do so (Bryman 2012, 393). These goals are showing in the objective of the study. One of the more concrete objectives was to generate better understanding for SMEs on how to protect against these cybersecurity threats and furthermore, spread the knowledge about the issues in the field of cybersecurity. Thus, in addition to generating theoretical contribution by conducting this research, the aim is also to generate practical contribution for increasing SMEs' cybersecurity levels.

Finally, the research process has followed four main areas of ethical principles (Bryman 2012, 135). First, it is assured that the research did not harm any of the participants involved in the research process. All interviewees participated voluntarily and their request for anonymity has been honoured. Additionally, all interview recordings and transcripts will be permanently deleted after five years after the thesis has been accepted and published. However, the personal data (names and contact information)

from the empirical data will be deleted already after the thesis has been accepted and thus, the data will be pseudonymized. Moreover, these personal data have only been used to contact the research participants to schedule the interviews and to discuss follow-up questions regarding the research with their own consent. In addition, the questionnaire, which results were not analysed in this research, was conducted anonymously by using Webropol.

Second, the principle of informed consent has been ensured by giving as much information as possible about the purpose and aim of the research to the interviewees. As mentioned, all interviewees participated voluntarily, and they were told more details about the research in the beginning of each interview. In addition, couple of interviewees asked to see the interview guide before the interviews were conducted which was provided to them prior to the interviews. Moreover, as mentioned previously, the finished version of the research paper and especially the results of the study will be offered to the research participants. Lastly, it is assured that neither invasion of privacy nor deception has occurred while conducting these interviews or during the whole research process.

5 RESULTS AND DISCUSSION

In this chapter, the findings from the empirical data have been introduced. The aim of this chapter, therefore, is to introduce plausible explanations to why the level of cybersecurity in Nordic SMEs varies. Moreover, the aim is to introduce suggestions based on the empirical findings on how these Nordic SMEs could improve their preparedness for cyber threats. In order to coherently present the results of the study, this chapter has been divided into three subchapters based on the more narrowly defined research questions posed in chapter 1.2. Thus, the results of the empirical findings have been presented in the following subchapters following the order of the research questions.

Chapter 5.1 presents the results from the empirical findings concerning different cyber threats that Nordic SMEs might encounter. Chapter 5.2, on the other hand, presents the results from the empirical findings that could explain why SMEs in the Nordic countries generally have not prepared for cyber threats. Lastly, chapter 5.3 presents the empirical findings regarding the opportunities on how these Nordic SMEs could improve their level of preparedness against cyber threats. Furthermore, the empirical findings are connected and analysed in the context of the theoretical framework introduced in chapter three.

5.1 Cybersecurity risks for Nordic SMEs

As mentioned in chapter 3.1 the first step of a risk management process is often the identification of risks (see figure 2). Therefore, in order to generate valid suggestions on how SMEs operating in the Nordic countries could improve their cybersecurity and cyber-resilience, it is crucial to understand the kind of threats these companies might encounter. Thus, the first research question posed in chapter 1.2 was formulated to study these threats. The empirical findings, additionally, showed evidence supporting the previous research (see chapter one) that in addition to larger organizations, cyber threats are in fact a serious threat for SMEs as well. This subchapter, therefore, presents the results analysed from empirical data regarding the possibility of SMEs encountering cyberattacks and the results for what kind of attacks these companies therefore are likely to encounter.

5.1.1 Motives behind cyberattacks targeted towards SMEs

In chapter one, it was concluded that according to previous research cyber incidents cause significant threats nowadays for SMEs as well. In fact, the Allianz Risk Barometer 2019 (2019, 22) ranked cyber incidents first in a list of top five business risks for SMEs. The results from the empirical findings support these findings. All six interviewees confirmed that cyberattacks are continuously targeted towards SMEs as well. The following quote from one of the interviews demonstrates this argument:

> *The attackers are not interested in who you are. They're walking there like elephants in a glass store. And if they happen to catch something on their net, they will rip off anything worth selling and that's it. And if not, they will just use your network for something else that's shady.* (Information Security Manager for a computer networking company)

The empirical findings suggest multiple reasons for targeting SMEs and, especially, strengthen the fact that being safe from cyberattacks as a smaller business, in fact, is a misconception. The results show various plausible explanations for why cyberattacks are, in addition to larger businesses, also directed towards SMEs. Understanding these reasons or motives behind cyberattacks that SMEs might encounter, is vital for understanding the importance of cyber risk management. In addition, as mentioned in chapter 3.2, understanding the motives for cyberattacks can help in the identification of cyber risks and consequently, assist in the whole cyber risk management process. Therefore, the motives for cyberattacks that emerged from empirical data are presented in this subchapter.

As mentioned earlier in chapter 1.1 and 3.2, the motives for cyberattacks are often related to financial gains or cyber-espionage (Getting defensive: how businesses can guard against cyberattacks 2019; Limnéll et al. 2014, 113). Additionally, as mentioned in chapters 1.1 and 3.2, motives for cyberattacks can also include e.g. political or military power gains, searching and mapping possible targets, revenge, aims to increase fear, attacker's renown or status seek, egoism, ideological motives etc. (Johnson 2016, 129-136; Limnéll et al. 2014, 113). The empirical findings, however, suggest that primarily the motives for attacking an SME consist of aims to achieve financial gains or cyber-espionage.

However, the study's results emphasize that it is important to be aware of these other motives since depending on the industry, for example, even an SME could encounter cyberattacks driven by other motives than just financial gains or cyber-espionage such as political motives, ideological motives or status seeking. The empirical findings suggest that generally these attackers could be labelled either as activists or indies. Typical targets of activists might include, for instance, fur farmers or companies associated with animal testing. Indies, on the other hand, are often labelled hackers in everyday language and could launch attacks to seek status within their community. Especially for SMEs working with controversial industries, it is important to note these, perhaps less common, motives for cyberattacks.

In addition to motives behind cyberattacks, the study's results suggest more general motives for why cyberattacks are nowadays targeted towards SMEs, in addition to larger organizations. The results of the study show that one reason behind the phenomenon is the automatization of the attacks. In addition to IT being largely automatized, the majority of cyberattacks are also nowadays automatized. Thus, it has become beneficial for the attackers to attack as many targets as possible at once, including SMEs. Before the development of automatization, these attacks were largely orchestrated manually. Therefore, in terms of economic motives, it might have been previously more cost-efficient to only target larger businesses. However, according to the results of the study, nowadays attackers can get a larger sample by attacking a large number of businesses at once and thus increase the possibilities of achieving the motives behind the attack.

According to the empirical findings, another explanation for cyberattacks being target towards SMEs lies in the simplicity of orchestrating a cyberattack. Due to the above-mentioned automatization these attacks have become less and less expensive. Furthermore, the results show that attackers might not even need special IT skills to plan a cyberattack since nowadays even cyberattacks can be purchased online. Evidently, anyone could, thus, plan and launch a cyberattack even without obtaining relevant experience or special IT skills.

In addition to automatization and simplicity of cyberattacks, the empirical findings, additionally, supported the argument from Tawileh et al. (2007, 332) about SMEs being the easiest point of entry into the system (see chapter 1.1). Therefore, SMEs can be used as means to expand the cyberattack vector and consequently, as paths to get access to a larger company. The empirical findings showed that whilst larger companies often collaborate somewhere along the supply chain with SMEs, it is plausible that the

weaknesses in cybersecurity of these smaller stakeholders can be exploited in order to gain access to a larger target organization. Thus, it seems that the old saying Tawileh et al. (2007, 332) also referred to, "a team or a system is only as strong as its weakest link", can very well be applied in the world of cybersecurity. Even if the larger company had ensured their cybersecurity, there might be a loophole somewhere in the supply chain, especially when collaborating with SMEs. In fact, the results of the empirical findings show that quite often the attacks bigger companies encounter result from weaknesses in a subcontractor's cybersecurity. Hence, it could also be argued that often attacking SMEs is easier than attacking larger organizations due to their tendency of having lower levels of cybersecurity.

All in all, as mentioned in chapters 1.1 and 3.2, there are several motives for attackers to launch cyberattacks, which most often are related to achieving financial gains or cyber-espionage. In addition, there are several reasons for why even SMEs are nowadays facing cyber threats. Therefore, it could be argued that the small size of the company and the thought of "I got nothing worth stealing" will not protect the company from becoming a potential target or victim of a cyberattack. Hence, by not only supporting the theories of cyberattack motives in previous research, the results of the study, additionally, provided explanations for why even SMEs might not be safe from cyberattacks. Moreover, understanding why SMEs might also end up as targets is crucial in order to understand the importance of including cyber risks into companies' risk analyses. However, in addition to understanding the motives behind why SMEs are at an equal risk of becoming targets of a cyberattack, it is important to also get a grasp on what kind of attacks SMEs might encounter. Hence, the next subchapter will introduce some of the most common cyberattacks SMEs might encounter based on the empirical findings.

5.1.2 Types of cyberattacks SMEs can encounter

Chapter 2.1 presented some notable cyberattacks that have received vast media coverage at the time writing this paper. The list included attacks such as ransomwares and data breaches. Even though the example cases presented in chapter 2.1 were all large MNCs, the empirical findings show that SMEs can often encounter very similar cyber threats. As mentioned in the previous subchapter, it is important to understand what types of cyber threats are common for SMEs. Additionally, in chapter 3.1 and 3.2 it was mentioned that one way to identify risks is to use existing risk registries (Pinto et al. 2015, 19; Refsdal et

al. 2015, 39-42). Hence this subchapter aims to list the most common cyber threats for SMEs based on the empirical findings at the time of writing this paper.

According to the empirical findings, cyberattacks can be roughly divided into four categories: destructive attacks, extortion, exploitation of the target's IT resources and stealing sensitive information or data. According to the study's results, the most common cyber threats for SMEs currently seem to drop into the second, third and fourth category. However, the first category can still be a valid threat and should not be bypassed. Figure 8 below summarizes these four categories of different cyberattacks that SMEs could encounter.

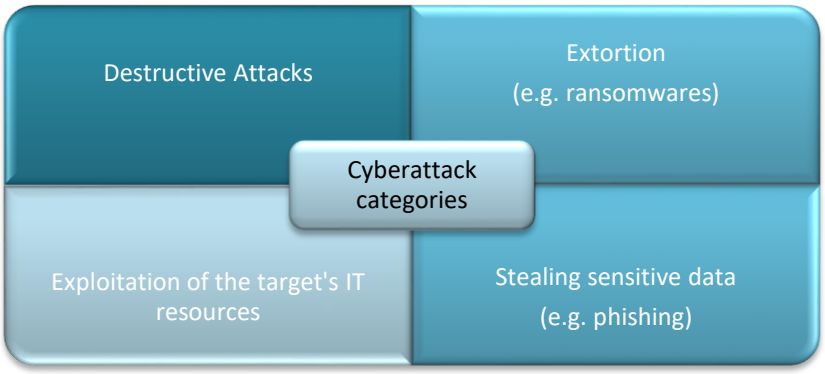

Figure 8 Cyberattack categories based on empirical findings

The first category of destructive attacks refers to cyberattacks where the attacker aims to disturb the business from continuing to operate. One example of a destructive attack is a denial-of-service (DoS) attack. These destructive attacks can be directed to, for example, computers, automation systems, IoT- based technologies etc. The study's results show that there can be multiple motives behind a destructive attack. Hence, these malicious cyber threats could be identified, as mentioned in chapter 3.2, by considering possible threat sources (Refsdal et al. 2015, 35) that might have motives to harm the business. Considering the risk assessment of destructive attacks, according to the empirical findings, the probability and consequences of encountering destructive cyberattacks generally depends on the industry the company is operating in as well as the level of dependability on information systems. For instance, a company that does animal testing might have a higher probability of encountering a destructive attack than a company which operates in a less controversial manner. In addition, let us assume that a business that sells sports equipment online would face a DoS attack. The attack could

harm the business quite drastically since the company's website could be down for a long time due to the attack and thus the consequences of the attack could be catastrophic. Hence, even if destructive attacks might generally be less common for SMEs to encounter, it is important that the company's contextual framework is taken into account when identifying and analysing these risks.

The second category of the types of cyberattacks, based on the empirical findings, includes attacks where the attackers use some type of extortion to achieve the intended outcomes. The most typical form of cyberattacks for SMEs in this category, based on the study's results, are ransomwares. As mentioned earlier in chapter 2.1, a ransomware is typically designed to encrypt files in a computer. After encrypting these files, the attacker typically demands payments in the form of cryptocurrencies for the files to be decrypted and recovered. Therefore, the motives are typically to achieve financial gains in the form of ransoms. According to the experts interviewed for this research, ransomwares have been quite popular in the past years even among SMEs. These ransomwares are most harmful for a company, if it has not continuously made back-ups. Thus, ransomwares highlight the importance of back-ups in any sized companies. Since the source of these extorting attacks can be rather difficult to detect, it is important to identify the assets and processes containing most vulnerabilities for these types of threats (see figure 6 in chapter 3.2).

The third category which represents a common threat for SMEs, according to the empirical findings, includes the exploitation of the target's IT resources. In practice, this often means that the target company's core business processes might slow down significantly if the capacity is partly or wholly used in operations to achieve the attacker's own motives. One example of a such attack would be a case where the attacker could be using the target's computing capacity to mine cryptocurrencies. Even though the consequences at first seem negligible, there are other threats concerned with these types of attacks. Once the wall is down and the attacker has gotten into the system, it becomes a lot easier to launch other types of cyberattacks, for example, to steal sensitive data. In addition, these types of attacks can, according to the study's results, often also be used as distractions while attacking the company some other way. The following quote illustrates this phenomenon:

> *These [attacks that exploit the target's IT resources] have certainly also been used merely as distractions where the attacker has actually done something entirely*

> *different than mined cryptocurrencies. Exactly so that the defender would think like "phew, we were in a luck since all this cost us was electricity usage".* (Global Technical Director and a "professional hacker")

The last category that rose from the study's results, referred to attacks that aim to steal sensitive data. Based on the empirical findings, the most common form of cyberattacks in this category are e-mail compromises (such as phishing attempts). The goal, according to the study's results, might be to steal client data, sensitive R&D data, or practically anything worth selling or knowing. According to the empirical findings, the type and amount of stolen data might vary significantly depending on the attacker and the target company. These types of attacks might then result, for instance, in data breaches and consequently, fines and penalties, damages on brand image and/or other financial losses depending on the type and amount of the stolen data. Hence, with these types of threats, a company could again focus on the assets and processes that contain significant and sensitive data and analyse the cyber vulnerabilities of these assets and processes (see figure 6 in chapter 3.2).

In addition to cyberattacks coming from external actors, the results show that it is rather common that cyberattacks in SMEs might also arise from inside the company. Furthermore, the study's results support the existing literature (Pinto et al. 2015, 7) in a sense that these cyberattacks can be either intentional or unintentional. The empirical findings suggest, additionally, that unintentional cyberattacks are perhaps more common than intentional cyberattacks among SMEs. In this context these unintentional attacks could perhaps rather be labelled as unintentionally caused vulnerabilities or cyber risks that might result in cyberattacks. The study shows that these vulnerabilities often result from unintentional mistakes that an employee has made merely because they were not aware of the consequences of the action leading to a cyber risk. In addition, the empirical findings show that in fact, quite often these unintentionally caused cyberattacks result from employees' responding to phishing attempts.

It is mentioned various times in this paper that the smaller size of the company is not associated with the smaller likeliness of becoming a target. However, the empirical findings do suggest that the industry in which the company operates in could play a role in the likelihood of becoming a target of a cyberattack depending on the type of the attack. Hence, it could be argued that the more the company relies on IT infrastructures and the more it needs to deal with sensitive data, the more it is likely to become a target of a

cyberattack. However, it has become a continuously growing trend that companies, regardless of the industry, nowadays rely on technical solutions and infrastructures. Hence, it remains for the company to analyse how much it depends on these IT infrastructures and thus, evaluate the risks' probability and consequences according to that dependability.

However, even if these types of threats might currently be the most common cyber threats for SMEs, it is crucial to note that the cyber world is extremely dynamic and new cyberattacks and attack vectors are created continuously. Thus, the dynamic environment creates the complexity of the phenomenon and it is safe to say that the plausible attacks are not limited to the four categories mentioned in this chapter. Thus, even by being aware of the cyber threats presented in this chapter today, it is not guaranteed that the company would be safe tomorrow. This in turn, highlights the importance of continuous strategy assessment as discussed in chapters 3.1 and 3.2 (see figure 2).

5.2 The level of cybersecurity in Nordic SMEs

As mentioned earlier in chapter 1.2, it became obvious quite early in the research process that generally SMEs have not adopted any cybersecurity strategies. Thus, the theoretical background and the empirical research was directed more towards the issue of why these companies generally have not prepared for cyber threats even when there is such strong evidence of the likelihood of cyberattacks being targeted towards SMEs and the severity of the consequences, as discussed in the previous subchapter and chapter 1. Therefore, this chapter presents the empirical findings to why Nordic SMEs have generally not adopted any cybersecurity strategies. In general, most of these findings seem to support the theoretical framework outlined in chapter 3.3.

The results of the study reveal two major reasons behind this lack of cybersecurity in Nordic SMEs. First major explanation seems to be the lack of awareness and the second explanation the lack of resources, most importantly financial capabilities. The following quote from one of the interviews illustrates these two points:

> *The biggest problems are money and the fact that the company is so deep inside their core business that they won't look at the big picture. Often, they don't have the understanding, knowledge nor business partners who would tell them that this [cybersecurity strategy] would be something*

> *worth doing.* (Information Security Manager for a computer networking company)

Therefore, the empirical findings in the context of Nordic SMEs align with the previous research presented in chapter 3.3. Hence, both these themes have been presented and discussed further in the following subchapters 5.2.1 and 5.2.2. In addition to low levels of awareness and limited resources, one larger theme that rose from the study's results was that the responsibility for cybersecurity tends to be poorly assigned or delegated inside Nordic SMEs. Hence, this theme is additionally discussed further in chapter 5.2.3. In chapter 3.3, awareness is introduced under the umbrella of limited resources. However, since all of the industry experts interviewed for this research emphasized the lack of awareness being a major challenge for Nordic SMEs, the theme has been introduced under a separate heading in this chapter.

5.2.1 *Awareness*

Based on the experts' experience and perception, the overall awareness of the importance of cybersecurity has slowly increased recently in the Nordics. However, the findings also showed that the relatively low level of awareness regarding cyber risks, especially among SMEs, is one of the main reasons for why Nordic SMEs generally have not prepared for these risks. Hence, the study's results seem to align with the previous research as discussed in chapter 3.3 (see, for example, Bada & Nurse 2019, 394; Tawileh et al. 2007, 332). The interviews revealed, for instance, that the experts still often run into the misconceptions also mentioned in chapter 3.3 (see, for example, Kurpjuhn 2015, 5; Kabanda et al. 2018, 270; Paulsen 2016, 92) of people in SMEs thinking that they are such small targets and have nothing worth stealing. Hence, the roots for why SMEs would not prepare for cyberattacks could, to some extent at least, be traced to the unawareness of the probability of encountering cyberattacks among SMEs. Consequently, the study's results show that this lack of awareness might result in direct vulnerabilities in companies' information systems.

Based on the empirical findings, it seems that without sufficient understanding in the managerial level and sufficient education of the employees, the risks for cyber incidents can increase exponentially. In chapter 5.1.2 it was concluded that one common type of cyberattack against SMEs is aiming to steal sensitive data from the company, for instance,

in the form of phishing attempts. These phishing attempts are an example of cyber risks where the likelihood of a cyber incident might increase significantly if the employees have not been educated and the level of awareness of cyber risks is low. Second practical risk that the study's results indicate was employees' tendency to easily switch to using personal email accounts to send sensitive information without even realizing that this data might be compromised by doing so. The following quote illustrates the problem regarding the lack of sufficient employee education and awareness:

> *The problem here is that even if we can fix bugs in software systems, patch them and make software repairs, we cannot make these software repairs to repair people's stupidity.* (Channel Director for a cloud data management company)

Third practical example resulting from unawareness regarding cybersecurity, has emerged after companies have shifted towards cloud usage. The study's results indicate a rather common misbelief among SMEs that data backups are not required after the data has been transferred to cloud services. In one of the interviews, the opportunities to storage huge amounts of data into cloud services were even referred to as being "catalysts" for even lower level of protection. According to the findings, nowadays more and more data has been using cloud services and due to the misconception, that the data would be safe in the cloud, it might be completely unprotected. This discovery refers to the same tendency mentioned in chapter 3.3 (Julisch 2013, 2208-2209), that companies tend to rely heavily on products' safety without creating their own cybersecurity strategies.

Hence, the lack of awareness seems to create chain reactions towards vulnerabilities and thus, low levels of cybersecurity. Based on the findings presented above, these chains appear to begin from the unawareness of cyber risks in the managerial level and thus, continue to unawareness in the employee level. This in turn seems to create vulnerabilities as a result of actions in day-to-day businesses which are not recognized as being risky.

However, the empirical findings also suggest that not all companies have completely ignored the risks concerning cybersecurity. Nonetheless, the study's results show that generally even if some SMEs have included cybersecurity in their risk analyses, the likelihood and severity of cyber risks are underestimated due to the misconceptions mentioned in the theoretical framework (see chapter 3.3 and for example Kurpjuhn 2015,

5; Kabanda et al. 2018, 270; Paulsen 2016; 92). Hence, the risk analysis might even be done, and thus, the risk might be approved seemingly and theoretically correctly due to the small likelihood of the risk. However, the plausible mistakes happen in the evaluation of the risks' likelihood and consequences since the empirical findings and the theoretical framework suggest that SMEs tend to especially underestimate the likelihood of these risks due to unawareness.

Evidently, based on previous research and study's results, it seems that quite often the low levels of cybersecurity can be traced to unawareness concerning cyber risks. Admittedly, it would be pointless to spend resources on cybersecurity if you are not aware that there is anything worth preparing for. Additionally, previous research indicated that generally risk management in SMEs is left for the manager or owner of the business (Boustras & Guldenmund 2017, 10). Hence, there might not be any justifications for creating a cybersecurity strategy if the managerial level of an SME is not aware of cyber risks potential likelihood and consequences. Therefore, in order to implement a suitable cybersecurity strategy, it might be necessary to start at the top of the company and first concentrate on the level of awareness regarding cybersecurity.

However, it is important to note that it is not the intention of this research to argue that all SMEs, without exceptions, would have limited knowledge about cybersecurity and every SME in the Nordics would underestimate the likeliness and consequences of cyber risks. This chapter is merely gathering plausible explanations based on empirical findings that might affect the state of cybersecurity in Nordic SMEs in a larger sense. Unfortunately, however, even being aware of the actual risks and consequences of cyberattacks, does not necessarily mean that the company would be prepared for such attacks. The study's results and the theoretical framework reveal other barriers, in addition to low levels of awareness, for creating cybersecurity measures in SMEs such as the lack of sufficient financial resources. Therefore, the challenge of limited resources will be discussed in the next chapter.

5.2.2 Lack of resources

As mentioned in chapter 3.3, the previous literature suggests that limited resources present one of the most crucial challenges for SMEs' cybersecurity (see, for example, Kaušpadienė et al. 2019, 979; Kabanda et al. 2018, 269; Tawileh et al. 2007, 332; Kurpjuhn 2015, 5). The empirical findings also indicated that these tight resources can be

considered as one of the most common reasons for why Nordic SMEs do not prepare for cyber threats. From the empirical findings two categories of resources, in addition to awareness, seem to stand out as being critical when considering the capabilities for creating cybersecurity strategies: financial resources and human resources.

Hence, even if awareness would be at a sufficient level for companies to understand the importance of cybersecurity, according to the study's results, the next issue is afterwards often the size of the budget and its flexibility. The results of the study show that perhaps the most defining attribute which makes the company decide whether it wants to protect itself against cyber threats, is the monetary costs of cybersecurity. As mentioned in the theoretical framework (see, for example Limnéll et al. 2014, 225; Tawileh et al. 2007, 332), cyber risk management often requires monetary investments, time investments, and investments in education of the staff. The following quote illustrates this problem:

> *The needs [for cybersecurity] are the same for every company out there. However, the size of the wallet is an extremely crucial determinant.* (Information Security Manager for a computer networking company)

According to the empirical findings, cybersecurity constitutes of two attributes: risk management and information security. This division of cybersecurity is similar to the division by Limnéll et al. (2014, 165-212) (see chapter 3.2) to strategical, operational and technical levels where the attribute of risk management refers to strategical and operational levels and the attribute of information security to the technical level. However, the study's results suggest that in many SMEs, cybersecurity is only seen as information security. Thus, it seems that the technical level of cybersecurity i.e. the information security is regarded as a completely separate issue and not as a part of the overall risk management of the company. Hence, SMEs might often see cybersecurity only as a cost instead of an investment in security. This view, or more generally these types of attitudes, could be, therefore, seen as a result of a mixture of both limited resources and limited awareness of the importance of cybersecurity.

The empirical findings, additionally, showed that even if a company is planning on investing in a new technology to improve its business operations, often cyber security and thus, information security of the new investment are bypassed (either forgotten or

knowingly ignored). The following quote indicates the problem that entrepreneurs often face:

> *The fact is that entrepreneurs are often extremely smart people. They're not stupid. It's just a question of having constantly more and more things to do and less time to do them. It leads to the need of having to prioritize. And then you just don't stop to think [about cyber security] because your focus needs to be in what you do and the products or services you're producing.* (Global Technical Director and a "professional hacker")

The quote above additionally illustrates the fact that SMEs often have to, additionally, operate with limited human resources. Due to these limited human resources, it seems according to the study's results, that SMEs might not have the ability to do risk management on strategical and operational levels. Instead, the study shows that SMEs tend to focus all resources they have on running the core business and fixing prevailing issues and challenges. Moreover, the study's results showed that there seems to be a significant shortage of qualified people in the field of cybersecurity overall. Thus, it is often difficult for even larger companies to find qualified employees to ensure companies' cybersecurity. Moreover, the empirical findings suggest that the entrepreneurs' expertise might concentrate on the product or service the company is producing and thus, creating risk management strategies might be out of the entrepreneurs' area of expertise.

5.2.3 Unclear responsibilities and the lack of cybersecurity governance

In addition to lack of awareness and limited resources, a third wider theme emerged from the empirical findings. This theme comprises the problem of not assigning the responsibility of cybersecurity for anyone inside the company. Multiple interviewees mentioned that rarely there is a person in an SME who would be responsible for cybersecurity and that these problems often start from the top management. This theme was also present in the theoretical framework and is referred in the previous literature (see, for example, Julisch 2013, 2210; Ilmonen et al. 2010, 165; Kabanda et al. 2018, 269-270) and in chapter 3.3 as lack of IT governance. However, in a larger sense, the phenomenon might be more appropriate to be referred to more generally as cybersecurity

governance. According to the empirical findings, IT in Nordic SMEs might be even governed to some extent or perhaps outsourced. However, according to the empirical findings, cybersecurity from the strategical and operational viewpoint is still generally often left ungoverned.

As mentioned, the study's findings suggest that the lack of cybersecurity governance starts from the top management. As mentioned in chapter 2.2, designating a data protection officer is not always mandatory. Legally the CEO has the responsibility of ensuring the company's cybersecurity and thus, cyber security can be easily neglected if the task has not been handled in the managerial level nor assigned to anyone else in the company. The empirical findings suggest that without clear responsibilities, these issues are often considered as someone else's responsibility and thus, not paid attention to. The following quote from one of the interviews illustrates this challenge:

> *The mindset is that "someone else will take care of this [cybersecurity] for me". That mindset should be abolished. That "someone else" doesn't exist unless you're willing to pay for it.* (Head of Cyber Security for a large MNC)

Even though this theme of cybersecurity responsibilities is here presented under a separate heading, it could be argued that it might be a result of the two other themes mentioned above. If the management is unaware of the need for cybersecurity or if there are very limited human resources (i.e. the staff has already their hands full with other operations), assigning the responsibilities of cybersecurity to someone in the company can easily be hindered.

All in all, according to the empirical findings, SMEs tend to face different challenges that lead to different levels of cybersecurity. After analysing these challenges, it seems that they all can affect one another and can also be affecting simultaneously on SMEs capabilities to prepare for cyber threats. For instance, let us assume that the company's top management is not familiar with plausible cyber risks. Therefore, the management level does not recognize the need for cyber risk management and has not assigned the responsibility for anyone in the organization. Additionally, all information security products are seen as additional costs rather than investments in security of the company. Even though some information security products or services might be implemented, they are regarded merely as obligatory costs and could even protect something else than the

company's most important assets if the company has not done an overall risk management strategy including cyber security. However, it is important to note that it is not assumed that universally every Nordic SME would face these same difficulties nor that every Nordic SME would have a poor cybersecurity strategy.

5.3 Improving the cyber security in Nordic SMEs

In chapter 3.2 it was mentioned that because cyber systems can have stakeholders and adversaries everywhere (Refsdal et al. 2915, 34-35), cybersecurity should not be regarded as separate phenomenon but rather as a contextual issue that is related to almost all other company operations (see figure 5). This argument was also supported by the empirical findings. For instance, the empirical findings suggest that in an organization, people are crucial players in understanding basic data security aspects such as strong passwords, data back-ups, phishing emails etc. From the process standpoint, on the other hand, organizations must understand the vulnerability of their processes to cyberthreats and plan how possible cyberattacks against processes would be dealt. Hence, it could be argued that cyber risk management should be present in the company's risk management as a whole as opposed to being regarded as an external event.

The most significant tool to increase the level of preparedness against cyber threats, according to the empirical findings, was the creation of cyber risk management strategy. Since most companies, even SMEs, have most likely at some point in time thought about their risk portfolios, it might only be a matter of adding the attribute of cyber security into the equation. The empirical findings suggest that once cybersecurity is regarded as risk management in addition to information security, the actual investments for cybersecurity can be understood and justified better.

Thus, the cybersecurity would start from the strategical level. As mentioned in chapter 3.2, according to Limnéll et al. (2014, 165-212) cyber security can be divided into three levels: strategical, operational and technical level. The study's results included advice on how SMEs could improve their cyber resilience in all these three levels. Therefore, this subchapter has been further divided in three parts according these levels of cybersecurity. The main focus will be on the strategical and operational levels which will be discussed in chapters 5.3.1 and 5.3.2. However, some advice related to the technical level will, additionally, be introduced in chapter 5.3.3.

However, before any strategical or operational improvements can be made, it is crucial that the awareness of cybersecurity increases among Nordic SMEs. Since in SMEs, the manager or owner of the business is often responsible in creating the company's risk management strategy, as mentioned in chapter 3.3, it is crucial that they are, at least to some extent, aware of plausible cyber threats and how these threats might affect the company's critical assets, resources and processes. Suggestions for how to increase this awareness, unfortunately, did not rise from the results of this research. However, it could be assumed that the more media coverage this issue receives, and the more nation states and professional industry groups spread knowledge about cybersecurity, the more the awareness ought to rise among SMEs. Nevertheless, the following chapter will represent the study's results on how SMEs could increase the level of cybersecurity strategically, operationally and technically. These chapters have also assisted in the iterative process of adapting the existing theories to the context of SMEs and thus, creating the theoretical synthesis in chapter 3.4.

5.3.1 Strategical improvements

As mentioned, after sufficient level of awareness, in order to improve the overall level of cybersecurity in SMEs, the study's results suggest by starting from making improvements on the strategical level. The empirical findings emphasize that the most important requirement for creating a cybersecurity strategy in a company or improving the level of cybersecurity, is the commitment of the top management. The findings show that without the commitment of the top management, it is extremely hard to implement any cybersecurity practices to the company since they often need financial investments. However, if the managerial level understands the need for cybersecurity, an SME can start the process of implementing cybersecurity strategy and culture into the company.

The experts' suggestions followed a rather similar pattern as the theoretical frameworks of operational risk management and cyber risk management in chapters 3.1 and 3.2. The study's results indicate that SMEs could start by identifying the company's strategical goals and their most critical assets. This is similar to the recognition of goals and objectives discussed in chapter 3.1 (see, for example, Pinto et al. 2015, 7-8; Ilmonen et al. 2010, 21-22). This step ought to be natural for SMEs since already in an early stage these companies often create a business plan. Business plan is a common starting point and often even necessary in order for a company to get financing, for instance. Business

plans often include preliminary SWOT analyses or risk analyses and hence, companies might have, to some extent, determined the company's critical resources, critical processes already in an early stage. However, the study's results underline that these critical assets and processes are often more than just tangible assets such as machinery. In fact, the empirical findings suggest that most important assets nowadays often consist of information and processes. In addition to recognizing the most critical assets, it is vital at this stage of the process to consider where they are located and who is using these assets. This first step of the process is vital in order for the company to know what needs to be protected.

The empirical findings supported the theoretical framework also in the next stage of the process, as the study's results showed that the next step would be to identify the risks associated with the critical assets. Since some SMEs might already have an existing risk portfolio, it might only be a matter of checking if the most crucial assets should include information/data and processes, but are not yet accounted for and therefore, extending the risk portfolio to also include cyber threats. As figure 5 in chapter 3.2 illustrates, cybersecurity is connected to almost all company operations and thus, often ought to be included in the risk portfolio one way or another.

In the stage of risk identification, the empirical findings also suggest on analysing which actors could potentially harm the company or the assets identified as critical. In theoretical framework this was referred to as identifying possible threat sources (Refsdal et al. 2015, 35). The results from the study suggest that threat sources that SMEs would mainly need to consider include cyber criminals and hackers. Also depending on the industry in which the company is operating in, it might be necessary to, additionally, consider activists as potential threat sources since the study's results show that the business environment and the industry significantly define which types of risks and threats the company has. The main point, however, is to position your company and the most critical assets to the environment of potential threats.

To conclude the study's results and theoretical framework regarding cyber risk identification, SMEs could facilitate the identification by using existing lists of possible cyberattacks such as the one created in chapter 5.1.2. In addition, after determining lists of most critical assets and processes, an SME could benchmark that list against a list of generally most vulnerable assets and processes to cyberattacks. An example of such list is illustrated in figure 6 in chapter 3.2.

Following the theoretical framework in chapters 3.1 and 3.2, the next step under scrutiny after identification of potential cyber risks is the assessment of these risks. As mentioned before, the risk assessment can often be a potential pitfall for SMEs due to limited knowledge about the likelihoods and consequences of different cyber risks. One practical advice from the industry experts to assess the consequences, was to make estimations first on how much that particular asset would be worth and second how long the company could survive if that particular asset would not be running smoothly or even if it was completely lost. As theoretical framework in chapter 3.2 suggests, once again existing lists from professional industry groups can help with evaluating the likelihood of the risks. In addition, as Ilmonen et al. (2010, 165) have mentioned it is often sufficient to only estimate the relative likelihood and consequences against other risks in this stage. After considering these aspects, it might be easier for an SME to form a risk assessment matrix as illustrated in figure 3.

5.3.2 Operational improvements

After conducting the above-mentioned strategical level of cyber risk management, risk identification and risk assessment, the process continues to the operational level. Like the theoretical framework, the empirical findings also suggested to next evaluate on how to treat these cyber risks. The theoretical framework in chapter 3.1 includes four approaches to treating these risks: elimination of the risk, mitigation of the risk, acceptance of the risk, and transfer of the risk (Ilmonen et al. 2010, 124). Considering SMEs limited resources, these companies might have to prioritize and concentrate on risks that have the highest relative probability and most catastrophic consequences. Due to the resource scarcity other risks might have to be accepted.

The study's results primarily focus on two treatment options: mitigation of the risk and transfer of the risk. Concrete examples on how to mitigate or transfer cyber risks are discussed more in subchapter 5.3.3. As mentioned in chapter 3.2, it is not optimal or even possible to create strategies to eliminate all possible cyber risks. However, it could still be assessed if there are some operations or day-to-day practices that clearly create vulnerabilities for critical assets or processes and that could easily be eliminated or replaced. An example of such practice could be, for instance, using personal e-mails for professional purposes. However, even if most cyber risks cannot completely be eliminated, based on the study's results, creating an optimal, context specific, cyber risk

management strategy that aims to mitigate or transfer the high-priority risks could be feasible even for SMEs despite the constraints mentioned earlier in chapters 3.3 and 5.2.

Furthermore, as the theoretical framework suggests, is important to audit the risk management strategy and to keep the strategy updated by assessing it regularly. These updates and continuous assessment of the critical assets and plausible threats is especially important considering the nature of continuously evolving cyber space. Therefore, the final suggestion to improve the operational level of cybersecurity in SMEs that rose from the study's results was to officially assign the responsibility of cybersecurity to someone inside the company and continuously measure or monitor that the issues of cybersecurity have been accounted for. Hence, it is, additionally, assured that there is someone responsible for the education of other employees. A sufficient cybersecurity governance, discussed in chapter 5.2.3, would also entail that the people inside the organization are managed considering the issue of cybersecurity.

Finally, the empirical findings suggest that first by concentrating on the improvements on the strategical level, the use of resources on cybersecurity becomes more justified and reasonable. Moreover, by concentrating on the improvements on the operational level, it will be easier to direct the available resources and operational tools for protecting the most crucial assets considering the continuity of the company's operations. These tools to improve SMEs technical level of cybersecurity will be discussed further in the next subchapter.

5.3.3 Technical improvements

The results of the study regarding possibilities on how to improve SMEs cybersecurity in practice can be divided in two risk treatment categories introduced in the theoretical framework: tools to transfer and tools to mitigate cyber risks. The study's results suggest cyber insurances as one practical and rather efficient way of transferring the cyber risks. This tool of using a cyber insurance might be the easiest option for some SMEs. According to the empirical findings these cyber insurances are a rather new concept in the Nordics. However, most big insurance companies seem to nowadays offer cyber insurances if the company decides that the optimal option would be to transfer the risk to an external party. However, even by transferring the risk by utilizing a cyber insurance, it is still important to note that data breaches, for instance, might cause significant harm

on the company's brand value. Hence, it might be worth evaluating which consequences can be tackled by transferring the risk, for instance, with a cyber insurance.

The practical methods on how to improve SMEs cyber resilience by mitigating cyber risks were discussed more extensively by the interviewees. One crucial method to increase cyber resilience, according to the study's results, was the education of the staff to increase awareness of the plausible risks and actions increasing these risks. Once the person responsible for cybersecurity has been assigned, they could be in charge of increasing the staff's awareness. This education can start from small improvements such as spreading the knowledge on what is a good password and educating the employees about the risks and characteristics of phishing e-mails. However, even if the responsibility of cybersecurity is assigned to one person, the study's results emphasize that a successful cyber resilience requires teamwork from the management and the employees of the company. The study's results also note that it is important to remember that technical solutions are never 100% sure because the end users can make mistakes which can increase risks of cyberattacks. Hence, the education and increasing the awareness are such important aspects in increasing the cyber resilience of an SME.

Nevertheless, the importance of IT solutions cannot be underestimated either and hence, the empirical findings suggested a few more technical solutions on how to mitigate cyber risks. The IT solutions that emerged from the empirical findings can be roughly divided into four categories: detective solutions, preventing solutions, patching or repairing solutions and recovering solutions. The detective and preventing solutions are proactive measures and designed to create the ability to detect possible threats and threat sources and prevent cyber risks from actualizing into cyber attacks. Whereas the repairing and recovering solutions are reactive measures to mitigate the consequences if the risk has already actualized and turned into a cyberattack.

Antivirus programs and firewalls represent examples of detective and preventing solutions which monitor plausible threats and threat sources. In addition to these, another quite practical emphasis that emerged from the empirical findings was the importance of data backups even if the company is using cloud services to storage data. In addition, according to the industry experts, it might be wise to technically limit the usability of critical systems to only actors who need these systems in their work. As an example, a company might want to limit access to sensitive and critical client data for only the employees who need this data in their daily operations.

Patching or repairing solutions and recovering solutions, on the other hand, are designed for increasing the company's ability to react fast if a cyber incident has been discovered. The study's results suggest on limiting the usability of the compromised system and creating a business continuum plan or a "plan b" in case a critical asset is compromised or lost. Again, regarding the recovering solutions, the experts emphasized the importance of backups. The following quote will illustrate the importance of this emphasis:

> *"That backup of yours is practically the only way you can survive from a ransomware attack without having to pay ransoms or starting all over"*
> (Security Offerings Architect for a large MNC)

Finally, the empirical findings emphasize that a cybersecurity strategy or improvements on the strategical and operational level alone are not enough. The strategy on paper does not ultimately help if the company has not additionally implemented measures on the technical level to increase the level of preparedness. Hence, a cyber security strategy should be regarded as a framework on what technical actions the company needs to implement to protect the most crucial assets from the most significant risks identified in the strategical level. In addition, nowadays, basic information regarding cybersecurity issues can be obtained rather easily from different sources such as publications from different industry groups, online articles from news media and private IT companies, as well as, from guidelines created by public (governmental) organizations. Examples of such guidelines have been drawn together in appendix 3 and will introduce even more detailed descriptions of practical measures that companies can implement in order to increase their cyber resilience.

In conclusion, the research problem was designed to study why the level of cyber security varies in Nordic SMEs and whether there would be room for improvements. The study's results, as well as previous research, indicate that the level of cybersecurity in Nordic SMEs generally is rather low although depending on the industry, there might be some exceptions as well. Nevertheless, the study's results show significant cyber risks regardless of the company's size. Thus, even SMEs might easily encounter cyberattacks. The empirical findings, as well as previous research, suggested multiple possible reasons for why SMEs typically might not have prepared for cyber threats. According to the study's results the most significant and common explanation seems to be the lack of

awareness among SMEs regarding the risks of becoming a target of a cyberattack. Moreover, attributes such as limited financial and HR resources and poor cybersecurity governance were introduced as reasons why SMEs could face difficulties in preparing for cyber risks even if they would actually recognize these types of risks' probability and severeness of the consequences.

As opposed to the other side of the research problem, the study's results suggested that there, in fact, might be room for improvements regardless of the challenges these companies tend to encounter. To conclude, the company would first have to recognize the importance of cybersecurity by being aware of the risks' probability and the plausible severity of the consequences. After this, the empirical findings could be divided into three categories of how to improve the company's cyber resilience: strategical, operational and technical tools. Strategical tools supported the theoretical framework presented in chapter three and focused on creating a cyber risk management strategy by identifying critical assets and risks and assessing the probability and consequences of these risks. The operational tools, on the other hand, included assessing and deciding on the methods used to treat these risks. Finally, technical tools included suggestions on how to improve company's cyber resilience in practice. These results were mainly used, in addition to the theoretical framework in chapters 3.1-3.3, to create iteratively the framework presented in chapter 3.4 which applies the theory and results of the study to suit the context of Nordic SMEs.

6 CONCLUSIONS

In the beginning of this paper it was mentioned that according to recent news articles the level of preparedness against cyber threats seems to vary significantly among companies. Therefore, the research problem was formulated to study the level of cybersecurity in Nordic SMEs and whether there would be room for improvements in these companies' cybersecurity strategies. Both previous research and the data gathered for this research implied that most SMEs have not adopted any cybersecurity actions. Thus, the research's focus was deepened to examine why these Nordic SMEs have not done so and what they could do despite these challenges. The study's results revealed various reasons for why the level of preparedness differs and why SMEs have generally not prepared for cyber risks. In addition, the results covered various suggestions on how that level of preparedness could be improved in strategical, operational and technical levels.

In this chapter, the study's findings are raised on a higher level and thus, the scientific and practical implications of conducting the research, have been discussed. First, as being a master thesis, subchapter 6.1 will present the scientific or theoretical contribution of the research. Hence, it aims to address how the study's results support the existing literature and theoretical framework. Additionally, the subchapter will introduce the plausible complements on the exiting theoretical framework and literature. Subchapter 6.2, on the other hand, presents the practical contribution this study's results offer. These practical contributions are mainly directed towards SMEs managerial level and thus, the subchapter is headed as managerial implications. Whilst the theoretical contributions are important from the academic point of view, the managerial implications additionally play an important role due to the normative nature and objectives of this research. Finally, subchapter 6.3 will address the limitations of this research and suggestions for further research.

6.1 Theoretical contribution

By contrasting the results of the study presented in chapter five against the theoretical framework presented in chapter three, it could be concluded that the study's results supported the existing research and theoretical framework. The main reasons why Nordic SMEs are not generally prepared for cyber threats included lack of awareness, lack of resources, and lack of cybersecurity governance. These three themes were also present in

the previous literature. Even though limited resources and lack of cybersecurity governance pose often significant challenges, the empirical findings especially emphasized the importance of awareness and understanding the need for cybersecurity. Hence, the empirical findings underlined the importance of awareness in order for companies to understand why it is important to create such risk management strategies and consider these strategies as investments rather than just obligatory costs. Only then, will it be possible to start improving a company's cybersecurity from the strategical, operational and technical levels.

Since the theory and the empirics of the study were formulated iteratively, it is rather difficult to distinct individual results from the empirical findings that would have increased the theoretical contribution. However, in chapter 1.1 it was mentioned that a few academic articles have referred to a research gap of how companies have integrated methods that add the level of cybersecurity. One theoretical contribution would, thus, be that the study's empirical findings suggested that at least in Nordic SMEs (when using the EU definition of an SME), companies have generally very low levels of cybersecurity. Although, there might be exceptions, for instance, due to stricter legislative requirements.

However, the most significant theoretical contribution of this research was the aim of applying the existing cyber risk management theories to the context of (Nordic) SMEs. Hence, due to the method of iteration, chapter 3.4 and especially table 1 have been created based on the existing literature and the results gathered from empirical findings. Therefore, the application of the cyber risk management model to suit the specific context of SMEs in table 1, could be seen as one of the most valuable theoretical contribution of this research. By gathering information from various academic publications and applying the findings from the empirical data, table 1 summarizes the process, difficulties and suggestions for improvements regarding cybersecurity in Nordic SMEs.

6.2 Managerial implications

One of the main objects of the research was to deliver practical contribution for SMEs operating in the Nordics. Hence, the practical contributions worked as a significant motive to conduct the entire research. Therefore, starting from the beginning, the research problem included the issue of whether there is room for improvements considering Nordic SMEs' cybersecurity. To facilitate this issue, the third research question was formulated as rather normative in nature and was aimed to deliver advice on how these SMEs could

actually increase their cyber resilience. Hence, chapter 5.3 introduced the results from the empirical findings on how Nordic SMEs could improve their level of cybersecurity.

In conclusion, the most significant issue and starting point for all improvements, according to the results of the study, was to increase awareness and knowledge around the phenomenon of cybersecurity. The misconceptions that cyber risks would be insignificant for SMEs due to their small size need to be abolished first. Therefore, the research also introduced the most common cyberattacks for SMEs and aimed to shed light on the probability of encountering cyber threats regardless of the size of the company and help the identification of plausible cyber risks. Once a sufficient level of awareness of the risks SMEs might encounter regarding cyber incidents has been achieved, it will be easier and more justifiable to concentrate on actions that would increase the level of cybersecurity in the company.

The study's results suggest beginning the improvements from the strategical level. By making a risk portfolio and analysis or including the dimension of cybersecurity to the company's existing risk portfolio and analysis, the company might be able to better protect its critical assets. One crucial aspect, the interviewees emphasized, was to notice that information or data and processes are quite often a part of a company's critical assets. This analysis, after all, forms the baseline for what to protect and where to prioritize, especially if the company is operating under limited resources as SMEs often are. In addition, the study's results emphasized the importance of assigning the responsibility of cybersecurity for someone inside the company (whether it is the CEO or another member of the top management or even an employee).

The more practical suggestions on the technical level included implementing both proactive and reactive solutions to protect the most crucial assets the company obtains. As an example of the reactive solutions, firewalls and antivirus programs were mentioned. In addition, the interviewees underlined the importance of spreading the awareness of cyber risks inside the organization in the form of educating the employees.

These guidelines form the study's results, represent the practical contribution of the research. In addition, other guides for further practical information have been referred to in chapter 5.3.3. Moreover, a few crucial points in the form of a short list on how to improve an SMEs cybersecurity have been summarized for SMEs' usage. This guide was attached to the questionnaire directed towards SME representatives which aimed to increase the data used to gather the results for this research. Even though the questionnaire did not generate enough answers in order to utilize them without hindering the

trustworthiness of the research, the questionnaire has still been opened 81 times. In addition, the list was published on different social media channels such as LinkedIn and Facebook to increase the practical contribution and usefulness of the study. The list was created before all the empirical data had been coded and thus, does not include all the information included in this paper. The list can be found translated from the appendices in this paper.

6.3 Limitations and suggestions for future research

As chapter four indicates, all methodological choices used in this research have been rationalized. Additionally, chapter 4.5 specifically addressed the trustworthiness and authenticity of this research. Moreover, in order to conduct this research, a significant number of existing publications were read and, additionally, referred to in this final paper. However, there are naturally limitations considering the research and thus, these limitations are addressed in this subchapter. Furthermore, suggestions for future research have been made from the perspective of the limitations this research contains.

First, it is important to note that this paper has not been written by an IT or information security expert and thus, most of the detailed practical solutions to increase cybersecurity have been left for the readers' responsibility and further reading. Therefore, the focus of this research is mainly on the managerial aspects of cybersecurity with some additions regarding technical improvements. In addition, it is important to remember that the nature of cyber threats is extremely dynamic and, unfortunately, criminals continuously find new ways to access organizations' networks remotely. Therefore, the information obtained from empirical findings and previous research reflect the time of writing this paper and might change in the future.

Moreover, as mentioned in chapter four, the study's results are not meant to be universally generalizable. Instead, the results aim to gather different cyber risks Nordic SMEs might encounter, different explanations for why Nordic SMEs could face difficulties in preparing for cyber risks, and different suggestions for how Nordic SMEs could improve their cyber security. Hence, the purpose is not to argue that all Nordic SMEs would face the same threats due to the same reasons leading to poor cybersecurity. Therefore, the results should be interpreted and applied by considering the contextual framework of the SME.

Another limitation this study contains, is that empirical data from SME managers or representatives could not be analysed to enrich the results. Additionally, this data would have worked as a supporting argument for the industry experts' perception that most SMEs generally do not prepare for cyber risks. Hence, this works as a suggestion for further research. As the industry experts noted, there are differences between different industries, for instance, due to regulative and legislative requirements. Therefore, it would be rather interesting to examine, perhaps quantitatively, if there are clear patterns of the levels of cybersecurity in SMEs depending on the industry the company is operating in. Furthermore, it could be studied whether there are industries where the level of cybersecurity among SMEs is low but the need for it, still high.

Moreover, as a suggestion for further research, it would, additionally, be interesting to study whether there are differences in what industry experts regard as sufficient level of cybersecurity and what SMEs regard as being prepared for cyber risks. Due to the challenges in awareness also mentioned in the results of this research, it could be possible that some SMEs might think they are prepared for cyber threats, however, the state of preparedness could be rather different if asked from an industry expert's analysis.

Finally, at the time of finishing this research, a Finnish SME that provides psychotherapeutic services ended up in news headlines after facing a significant data breach where patients' sensitive information was stolen and leaked (Rinta-Jouppi 2020). Additionally, the hacker had claimed the CEO to pay bitcoins as ransoms (Rinta-Jouppi 2020). At the time of finishing the research process the case had seemed to have received quite a lot of media coverage and people in social media have shown support for the victims of the data breach. Hence, for further research, it would be interesting to see if this case, or cases regarding SMEs' cyberattacks in the media in general, would have a positive effect on the awareness of cyber risks among SMEs.

7 SUMMARY

The contemporary business world is driven by technology. Thus, companies are depending more and more on technological solutions in their daily operations. Along with the advantages and opportunities of the use of technological solutions, new threats have, however, risen in the form of cyber threats. The importance of cybersecurity has grown significantly and both, previous research, and the study's findings prove that the size of the company does not affect the probability of becoming a target of a cyberattack. Previous literature and the empirical findings proposed multiple motives behind cyberattacks and most commonly these motives seem to be related to achieving financial gains or cyber-espionage. Even though there are different motives for cyberattacks, the consequences, regardless, might often include significant monetary losses.

As opposed to general misconceptions, this research indicates that even SMEs are likely to encounter cyber risks and the consequences, such as financial costs, can be significantly high even for SMEs especially if mirrored against their annual revenues. Nevertheless, according to previous research and empirical findings, it seemed that the level of cybersecurity in SMEs is generally quite low despite the likelihood and significance of the consequences of cyber risks. In addition, the existing literature and research on cybersecurity seemed to concentrate on bigger companies and thus, were rather limited in the context of SMEs. Therefore, this research was directed to examining the level of cybersecurity in Nordic SMEs. The objective was to develop theoretical contribution to the process of cyber risk management in the context of SMEs and practical contribution in the form of managerial implications for how Nordic SMEs could improve their cybersecurity.

The theoretical framework used in this research concentrated on operational risk management, cyber risk management and the challenges SMEs encounter regarding cybersecurity that have been identified in previous literature. Since cybersecurity is a part of organizations' risk management strategies, operational risk management offered first a wider scope to the generalities and practices of risk management. Consequently, cyber risk management offered a more detailed framework of the risk management strategy process in the context of cybersecurity. Operational risk management and cyber risk management theories, therefore, presented the general path and steps for (cyber) risk management (see figure 2). These general steps were utilized later in the analysis of applying the theoretical framework with the use of empirical findings to the context of

SMEs. However, in order to apply the theories to the context of SMEs, it was first important to understand what difficulties these companies encounter that might hinder their preparedness for cyber threats. Hence, the theoretical framework also included the cyber risk management challenges for SMEs gathered from existing literature which were mostly related to awareness and attitudes, limited resources and the lack of IT governance. Finally, based on the theoretical framework mentioned above (and in chapters 3.1-3.3) and the results of the empirical findings, the theoretical synthesis in chapter 3.4 was drawn iteratively to apply the models of cyber risk management to the context of SMEs.

The research was based on subjectively constructivist and interpretivist paradigms. These ontological and epistemological assumptions, thus, created the framework for the entire study and therefore, the research was conducted qualitatively by conducting semi-structured interviews with six industry experts. The process of the research progressed iteratively and thus the theoretical framework and empirical findings were gathered simultaneously. The results from the empirical data gathered from the semi-structured interviews were first transcribed and then coded in order to analyze the results. In addition, the quality of the research has been addressed and ensured by addressing different evaluation criteria for trustworthiness and authenticity.

The results of the research have been divided into three parts following the structure of the research questions. Regarding the first research question, the empirical findings supported the previous research by concluding that it is, in fact, rather common that also SMEs nowadays encounter cyberattacks. In addition, the study's results offered several motives for why SMEs are nowadays targeted in addition to larger organizations. These motives included, for example, automatization, simplicity of cyberattacks and the fact that SMEs are often easier targets. In addition, as previous literature suggests, the study's results show that primarily the motives for attacking an SME consist of aims to achieve financial gains or cyber-espionage. Therefore, the study's results showed three categories of most common cyberattacks for SMEs: extorsion attacks (such as ransomwares), attacks that aim to steal sensitive data (such as phishing attempts) and attacks that exploit the target company's IT resources. However, the study's results emphasize that depending on the contextual framework of the company, it is important to be aware of other motives and types of attacks as well.

Regarding the second research question, the study's results indicated that the most common reasons for why SMEs might not have prepared for cyberattacks include the lack of awareness, limited financial and human resources, and lack of cybersecurity

governance. From the empirical findings, it could be concluded that all these above-mentioned reasons can affect one another and could also be affecting simultaneously on SMEs capabilities to prepare for cyber threats. These results were mainly in line with the theoretical framework although the empirical findings seemed to explicitly stress the importance of awareness as a hindering attribute for SMEs cybersecurity.

Finally, regarding the third research question, the study's results indicated different normative suggestions on how to improve the level or cybersecurity in Nordic SMEs. These suggestions were divided into three levels: strategical, operational and technical level. Strategical and operational level suggestions followed the theoretical framework by adapting the different phases of cyber risk management to the context of SMEs. The technical level suggestions, on the other hand, presented more practical tools on how to improve the level of cybersecurity in Nordic SMEs. These results of the study were used to apply the existing theories in cyber risk management to suit the context of SMEs thus, representing the theoretical contribution of the research. In addition, the results regarding the threats these Nordic SMEs might encounter and how they could improve their cybersecurity can be regarded as practical contribution of this research.

REFERENCES

Allianz Global Corporate & Specialty SE (2019) *Allianz Risk Barometer 2019*. <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf>, retrieved 17.11.2019.

Bada, M. – Nurse, J. (2019) Developing cybersecurity education and awareness programmes for Small and medium-sized enterprises (SMEs). *Information and Computer Security*, Vol. 27 (3), 393–410.

Banks, E. (2004) *Alternative risk transfer: Integrated risk management through insurance, reinsurance, and the capital markets.* John Wiley & Sons Inc., NY.

Basel Committee on Banking Supervision (2011) *Principles for the Sound Management of Operational Risk.* <https://www.bis.org/publ/bcbs195.pdf>, retrieved 15.3.2020.

BBC (2019, July 8) *British Airways faces record £183m fine for data breach.* <https://www.bbc.com/news/business-48905907>, retrieved 18.11.2019.

BBC (2020, March 11) *Coronavirus confirmed as pandemic by World Health Organization.* <https://www.bbc.com/news/world-51839944>, retrieved 19.10.2020.

Boustras, G. – Guldenmund, F. (2017) *Safety management in small and medium sized enterprises (SMEs).* CRC Press.

Bryman, A. (2012) *Social research methods*. Oxford University Press Inc., New York.

Cassell, C. – Symon, G. (2004) *Essential Guide to Qualitative Methods in Organizational Research. In Essential Guide to Qualitative Methods in Organizational Research.* SAGE Publications.

Chen, P. – Kataria, G. – Krishnan, R. (2011) Correlated Failures, Diversification, and Information Security Risk Management. *MIS Quarterly*, Vol. 35 (2), 397–422.

Cisco (2020) *What Is Cybersecurity?* <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>, retrieved 15.2.2020.

Council of the European Union (2016, April 6) *Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=consil:ST_5419_2016_INIT>, retrieved 18.4.2020.

D O'Gorman, K. – MacIntosh, R. (2014) *Research Methods for Business and Management: A Guide to Writing Your Dissertation.* Goodfellow Publishers, Limited.

Deloitte & Touche LLP. (2019) *The future of cyber survey 2019.* <https://www2.deloitte.com/za/en/pages/risk/articles/2019-future-of-cyber-survey.html>, retrieved 17.11.2019.

Eriksson, P. – Kovalainen, A. (2016) *Qualitative Methods in Business Research: A Practical Guide to Social Research.* Sage Publications Ltd.

Europa (2017) *What is an SME?* <https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_fi>, retrieved 18.11.2019.

Europa (2020) *Data protection under GDPR.* <https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm>, retrieved 26.5.2020.

EY (n.d.) *Tietosuoja-asetus.* <https://www.ey.com/fi/fi/services/tietosuoja>, retrieved 18.11.2019.

Fenz, S. – Heurix, J. – Neubauer, T. – Pechstein, F. (2014) Current challenges in information security risk management. *Information Management & Computer Security,* Vol 22 (5), 410-430.

Forbes (2018, November 30) *Marriott Breach -- What Happened, How Serious Is It and Who Is Impacted?* <https://www.forbes.com/sites/kateoflahertyuk/2018/11/30/marriott-breach-what-happened-how-serious-is-it-and-who-is-impacted/#80552627d25a>, retrieved 17.11.2019.

Guba, E. – Lincoln, Y. (1994) Competing paradigms in qualitative research. *Handbook of qualitative research,* Vol. 2 (163-194), 105.

Haimes, Y. (2016) *Risk modeling, assessment, and management* (4th ed.). John Wiley & Sons Inc., Hoboken, N.J.

Heikkilä, J. (2020, March 12) *Koronavirus on eristänyt miljoonat työntekijät koteihinsa: Etätyöskentely kodin turvasta aiheuttaa kuitenkin uuden uhan.* <https://www.mtvuutiset.fi/artikkeli/koronavirus-on-eristanyt-miljoonat-tyontekijat-koteihinsa-etatyoskentely-kodin-turvasta-aiheuttaa-kuitenkin-uuden-uhan/7758332#gs.4f1gnm>, retrieved 19.4.2020.

Hiscox (n.d.) *The Hiscox Cyber Readiness Report 2019*. <https://www.hiscox.co.uk/cyberreadiness>, retrieved 16.3.2020.

Hyppönen, M. (2020, April 1) *Webinar: Cyber Security and COVID-19. F-secure.* <https://www.f-secure.com/en/business/events/cyber-security-and-covid-19>, retrieved 21.4.2020.

Ilin, T. – Varga, L. (2015) The uncertainty of systemic risk. *Risk Management*, Vol. 17 (4), 240–275.

Ilmonen, I. – Kallio, J. – Koskinen, J. – Rajamäki, M. (2010) *Johda riskejä: käytännön opas yrityksen riskienhallintaan*. Tammi, Helsinki.

Johnson, M. (2016) *Cyber crime, security and digital intelligence*. Routledge.

Julisch, K. (2013) Understanding and overcoming cyber security anti-patterns. *Computer Networks*, Vol. 57 (10), 2206–2211.

Kabanda, S. – Tanner, M. – Kent, C. (2018) Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269-282.

Kaušpadienė, L. – Ramanauskaitė, S. – Čenys, A. (2019) Information security management framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy*, *25*(5), 979–997.

Kendrick, R. (2010) *Cyber risks for business professionals a management guide*. Ely: IT Governance Pub.

Klapkiv, L. – Klapkiv, Y. (2018) Methods for the identification of cyber risks: an analysis based on patent data. *CBU International Conference Proceedings.,* Vol. 6, 241–46.

Kok, J. – Boers, E. – Kosters, W. – Van der Putten, P. – Poel, M. (2009) Artificial intelligence: definition, trends, techniques, and cases. *Artificial intelligence*, 1.

Kovácsné Mozsár, A. – Michelberger, P. (2018) IT risk management and application portfolio management. *Polish Journal of Management Studies*, Vol. 17 (2), 112–122.

Kurpjuhn, T. (2015) The SME security challenge. *Computer Fraud & Security*, *2015*(3), 5-7.

Lam, J. (2014) *Enterprise Risk Management : From Incentives to Controls*. John Wiley & Sons Inc., Hoboken, N.J.

Lepistö, J. (2019, September 4) *Kyberrikollisuus on kasvanut miljardien eurojen globaaliksi bisnekseksi: "Varmasti ohittaa jossain vaiheessa jopa huumekaupan"*. <https://www.mtvuutiset.fi/artikkeli/kyberrikollisuus-on-kasvanut-miljardien-eurojen-globaaliksi-bisnekseksi-varmasti-ohittaa-jossain-vaiheessa-jopa-huumekaupan/7534780#gs.479lpm>, retrieved 16.9.2019.

Lex Access to European Union law. (n.d.). *2AD*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX:02016R0679-20160504>, retrieved 18.11.2019.

Limnéll, J. – Majewski, K. – Salminen, M. (2014) *Kyberturvallisuus*. Docendo Oy, Jyväskylä.

Lincoln, Y. – Guba, E. (1985) *Naturalistic inquiry*. Sage, Newbury Park, CA.

Merriam-Webster (n.d.) <https://www.merriam-webster.com>, retrieved 26.5.2020.

Mukhopadhyay, A. – Chatterjee, S. – Bagchi, K. – Kirs, P. – Shukla, G. (2019) Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers*, Vol. 21 (5), 997–1018.

Nam, T. (2019) Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*, 101122.

New York Times (2018, September 28) *Facebook Security Breach Exposes Accounts of 50 Million Users.* <https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html>, retrieved 17.11.2019.

Nycz, M. – Martin, M. – Polkowski, Z. (2015) The cyber security in SMEs in Poland and Tanzania. In *2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. AE-27). IEEE.

Oxford Learner's Dictionary (n.d.) <https://www.oxfordlearnersdictionaries.com>, retrieved 17.11.2019.

Paulsen, C. (2016) Cybersecuring Small Businesses. *Computer*, *49*(8), 92–97.

Pinto, C. – Magpili, L. – Jaradat, R. (2015) *Operational risk management*. Momentum Press, New York, NY.

Purdy, G. (2010) ISO 31000:2009—Setting a New Standard for Risk Management. *Risk Analysis*, Vol. 30 (6), 881–886.

Rees, L. – Deane, J. – Rakes, T. – Baker, W. (2011) Decision support for Cybersecurity risk planning. *Decision Support Systems,* 51(3), 493-505.

Refsdal, A. – Solhaug, B. – Stølen, K. (2015) *Cyber-risk management*. Springer, Cham.

Rinta-Jouppi, A. (2020, October 21) *Sadan psykoterapiapotilaan arkaluontoisia tietoja on vuodettu verkkoon, poliisi tutkii asiaa – Hakkeri vaati yli 400 000 euroa ja väittää varastaneensa kymmeniä tuhansia potilastietoja.* Kauppalehti. < https://www.kauppalehti.fi/uutiset/sadan-psykoterapiapotilaan-arkaluontoisia-tietoja-on-vuodettu-verkkoon-poliisi-tutkii-asiaa-hakkeri-vaati-yli-400000-euroa-ja-vaittaa-varastaneensa-kymmenia-tuhansia-potilastietoja/41c7a931-72a4-4a29-8cd8-7df330d77a73>, retrieved 29.10.2020.

Rittinghouse, J. – Hancock, B. (2003) *Cybersecurity operations handbook*. Elsevier Digital Press, Amsterdam.

Rubio, J. – Alcaraz, C. – Roman, R. – Lopez, J. (2019) Current cyber-defense trends in industrial control systems. *Computers & Security,* 87, 101561.

Saleh, M. – Alfantookh, A. (2011) A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, Vol. 9 (2), 107–118.

Sangster, K. (2020, August 5). *COVID-19 leads to surge in cyberattacks.* <https://uk.finance.yahoo.com/news/covid-19-leads-to-surge-in-cyberattacks-144142232.html?guccounter=1>, retrieved 24.8.2020.

Steinberg, S. (2020, March 9) *Cyberattacks now cost companies $200,000 on average, putting many out of business.* <https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html>, retrieved 16.3.2020.

Symantec (2017, October 23) *What you need to know about the WannaCry Ransomware.* <https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack>, retrieved 17.11.2019.

Symantec (2017, October 24) *Petya ransomware outbreak: Here's what you need to know.* <https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper>, retrieved 17.11.2019.

Tawileh, A. – Hilton, J. – Mcintosh, S. (2007) Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. In: *ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference*, 331–339.

The Telegraph (2019, August 12) *Getting defensive: how businesses can guard against cyberattacks.* <https://www.telegraph.co.uk/business/tips-for-the-future/smes-guard-against-cyberattacks/>, retrieved 16.3.2020.

Uber (2017, November 21) *2016 Data Security Incident.* <https://www.uber.com/newsroom/2016-data-incident/>, retrieved 17.11.2019.

United States Government Accountability Office (2018, August) *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach.* <https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf>, retrieved 17.11.2019.

UpGuard (2020) *What is an Attack Vector? Common Attack Vectors.* UpGuard. <https://www.upguard.com/blog/attack-vector>, retrieved 15.3.2020.

UpGuard (2020) *What is a Cyber Threat?* UpGuard. <https://www.upguard.com/blog/cyber-threat>, retrieved 15.3.2020.

Vincent, N. – Higgs, J. – Pinsker, R. (2017) IT governance and the maturity of IT risk management practices. *Journal of Information Systems,* Vol. 31 (1), 59–77.

WHO (2020, April 17) *Coronavirus disease (COVID-19).* <https://www.who.int/news-room/q-a-detail/coronaviruse-disease-covid-19>, retrieved 19.10.2020.

Wortmann, F. – Flüchter, K. (2015) Internet of Things. *Business & Information Systems Engineering*, Vol. 57 (3), 221–224.

Yannakogeorgos, P. – Lowther, A. (eds.) (2013). *Conflict and cooperation in cyberspace: The challenge to national security.* CRC Press.

APPENDICES

APPENDIX 1 OPERATIONALIZATION TABLE

RESEARCH PROBLEM	RESEARCH QUESTIONS	THEORY	THEMES/INTERVIEW QUESTIONS
The state of cybersecurity in Nordic SMEs: why it varies and are there room for improvements concerning preparedness for cybersecurity threats?	*What are the cybersecurity risks for SMEs operating in the Nordic countries?*	Cyber risk management: Risk identification (Refsdal et al. 2015)	1. What is your job like and what kind of background do you have related to cybersecurity and IT industry? 2. What type of businesses do you have experience working with related to cybersecurity issues? 3. What type of cyber threats do Finnish/Nordic companies face? 4. Are these threats similar regardless of the size of the company? 5. What kind of cyber threats would be plausible for SMEs? 6. Are cyber threats similar regardless of the industry the company is operating in? 7. What kind of consequences these threats might have on the business operations? (assuming

			that the company is somehow depending on technology)
	Why SMEs operating in the Nordic countries don't prepare against cybersecurity threats?	Different articles and books. See chapter 3.3 for more detailed references.	1. How do you think Finnish (SMEs) are prepared for cyber threats? 2. Are there differences or similarities compared to other Nordic countries in terms of the level of preparedness? 3. Should SMEs prepare for cyber threats better? 4. Why do you think SMEs have not prepared for cyber threats?
	How could SMEs prepare for cybersecurity threats?	Operational risk management & Cyber risk management	1. Why do you think SMEs should prepare for cyber threats? 2. What kind of tools/procedures SMEs could use to better prepare for cyber threats? 3. What are the reasons why a Nordic SME would decide to invest in cybersecurity.

APPENDIX 2 QUESTIONNAIRE ATTACHMENT

Answering the questionnaire lasts approximately five minutes. All answers will be handled anonymously, and the answers will be used in a master thesis that concentrates on SMEs preparedness against cyber threats.

Most common cyber risks for SMEs:

- Phishing
    - Method that attackers use in order to gather classified information such as credit card information, usernames, passwords etc.
    - Often the attacker will present himself as a trustworthy person from the receiver's point of view and asks them to open an e-mail or other message that often includes a link or an attachment.
    - These messages can seem surprisingly trustworthy and believable
- Malware
    - Might, for example, edit or collect data/information from a computer or hijack the computer
- Ransomware
    - The criminal often threatens to encrypt the data they have accessed or publish it. Therefore, the targeted company cannot access their own data anymore.
    - As ransoms, the attacker often requires cryptocurrency such as Bitcoins
- Crypto jacking
    - The attacker hijacks your computer to mine cryptocurrencies
    - It requires quite a lot of computing capacity to mine cryptocurrencies. Hence, the performance of your computer might weaken significantly
- Data breaches
    - Due to the current legislation, data breaches can cause significant fines for the company under the attack
- IoT Attacks
    - In addition to computers and tablets, even more devices are now connected to networks (such as Wi-Fi routers, web cameras, smart watches, industrial equipment, cars etc.)

    - Accessing these devices enables weakening their performance or shutting down systems entirely
- Distributed Denial of Service Attack
    - The attacker can take in control many devices and networks, for instance, to overheat the demand. This, in turn, can cause your web pages going down

Ways to protect from these risks:

- Analyse the goals and objectives of your company and the risks and threats connected to these goals and objectives
    - Think how many devices your company uses that are connected to networks
    - Remember that the size of the company is not nowadays connected to the probability of becoming a target of a cyberattack → try to base your risk analysis on facts rather than perceptions
- Delegate or take the responsibility of cybersecurity
    - You can easily find more information and tips on the internet regarding cybersecurity
- Education of the staff to be careful
    - Always remember to check carefully, for instance, the e-mail address of the sender (it might be very similar to the actual e-mail address)
    - Change passwords regularly and keep in mind the strength of the password
- Remember to regularly make backups from your data, even if you use cloud services to storage the data
    - Note that using cloud services, does not replace the need for backups
- Usually paying ransoms in case of a ransomware attack won't help. The data might be already lost regardless.
    - Notify the authorities. You can make a police report electronically or at your nearest police station.
    - If you become a victim of a cyberattack, contact companies offering cybersecurity services and expertise
- Most insurance companies also offer cyber insurances nowadays (find under cyber insurance or information security insurance or ask about it from your insurance company)

In case you want further information or information about the sources or studies regarding the subject or other information regarding my master thesis, I will gladly answer your questions via e-mail (jonna.j.reilimo@utu.fi). Good luck and stay healthy!

APPENDIX 3 FURTHER READING & USEFUL WWW-LINKS

Europol. *Public awareness and prevention guides.* <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides>.

Kauppakamari (2019, September 27). *Yrityksiin kohdistuvat kyberuhat 2019.* <https://helsinki.chamber.fi/wp-content/uploads/sites/2/2020/01/yrityksiin-kohdistuvat-kyberuhat-2019.pdf>. (Available only in Finnish)

National Cyber Security Centre (2018, November 17). *10 steps to cyber security.* < https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps>.

Traficom (2020). *Pienyritysten kyberturvallisuusopas*. <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf >. (Available only in Finnish)