FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study programme / specialisation: Risk Analysis and Governance	The *spring* semester, *2023* Open
Author: Luka Pejic	
Supervisor at UiS: Lasse Berg Andersen	
Thesis title: Cybersecurity in small and medium-sized enterprises	
Credits (ECTS): 30	
Keywords: Cybersecurity, risk, risk analysis, risk perception, risk science, SME, ISO 27001, cyberattack, information security	Pages: 54 Stavanger, *15. 06. 2023*

Preface

After many exams, assignments, lectures, and group projects it came time to put in one last effort to obtaining a master's degree in Risk Analysis and Governance.

This master's thesis is a final chapter of a two year, challenging, but exciting period of my life.

First of all, I would like to thank all of the lecturers that I have had the opportunity to meet during these past two years at the University of Stavanger. I would also like to thank my family and friends for their unconditional support during this process.

I also want to send a big "thank you" to my workplace for always adapting to my circumstances and making it easier for me to direct my focus on the studies when I needed it.

And of course, I would like to thank my supervisor Lasse Berg Andersen who has always been pushing and motivating me to finish this thesis to the best of my abilities.

Luka Pejic

Stavanger, 15. June 2023.

Abstract

As technology is evolving so is the cybercrime, there are new tools and techniques for cyberattacks being developed continuously (Bendovschi, 2015, p. 24). Every business, no matter what size it is, faces some form of digital threat every day. Without knowledge about these threats a business can very quickly find itself in a tough situation with consequences that can shut down a business for good in a matter of hours. The digitalization has progressed quickly and may have created room for threats that we don't necessarily have control over. A couple of very simple cybersecurity measures can sometimes be a deciding factor in preventing a cyberattack. The aim of this thesis is to discover how significant the cybersecurity risks are for SMEs (small and medium-sized enterprises), whether the SMEs are aware of these risks, and to present a framework which can help SMEs incorporate a strategy to manage cybersecurity risks.

The most common causes of a successful cyberattack in SME sector are based around not having enough competence or technical tools in this field. Not only does successful cyberattack affect a business financially, but usually also comes with reputational damage if the case of a cyberattack was to go public. In addition, through the eyes of cyber criminals SMEs are seen as an easy target since attacking these organization brings in hardly any attention of media or law enforcement. The SMEs are therefore completely on their own in this battle, and therefore need to take responsibility themselves instead of allowing their "fate to rest on someone else's hands". There can be seen a slight increase in awareness towards cybersecurity risks, but not nearly as much as it should be considering how impactful these risks can be. It is very difficult to say for sure what the reason behind it is, but it seems that the lack of "talk" about successful cyberattacks in the business world contributes to it greatly. But on the other hand, it is understandable that businesses won't go public with information about being targeted by cyber criminals since everyone wants to keep their reputation intact.

This thesis offers a framework which SMEs can use to build a resilient system against cybersecurity risks. The framework that is presented also addresses the challenge most SMEs have which is very limited resources to devote to cybersecurity. Therefore this framework offers a simple process which can benefit an organization significantly. The framework incorporates risk science and is inspired by an international standard for information security management and emphasizes three key points which can point an organization in the right direction: risk assessment, leadership, and employee awareness and training.

Table of contents

List of figures

1.0 Introduction

1.1 Research background

While cybercrime towards SMEs is increasing it is important to be mindful of the risks it brings and act accordingly (Rahmonbek, 2023). Based on the 2023 UK Government's cybersecurity breaches survey, 31% of 1387 micro businesses (1 to 9 employees) and 32% of 400 small businesses (10 to 49 employees) have identified cyber breaches or attacks in the last 12 months (DSIT, 2023). With 79%, phishing attacks are the most common types of breaches or attacks among those that have experienced an attack in the last 12 months (DSIT, 2023). There has also been a decline in breaches or attacks for micro and small businesses, which went down from 36% and 46% in 2022 to 31% and 32% in 2023 (DSIT, 2023). A reason for this may be that there is a reduction in cyberattacks, but this doesn't add up with what large businesses are experiencing, as they are experiencing a rise in cyberattacks, but on the other hand it could be that cyber criminals are turning away from smaller organizations (DSIT, 2023). There is also a possibility that smaller organization are less likely to identify breaches or attacks in comparison with previous years, which could be because of internal factors such as fall in logging and monitoring activity or lower prioritization of cybersecurity (DSIT, 2023).

In some of the interviews performed by the Department for Science, Technology and Innovation, we can see some of the challenges that smaller organizations are facing, such as heavily relying on digital service providers when it comes to cybersecurity (DSIT, 2023). Multiple organizations have expressed that they would go to these providers for advice and guidance in case of an accident, it also seems as if these organizations have assigned all responsibility for cybersecurity to their digital service providers and therefore did not feel any need to establish internal processes for cybersecurity (DSIT, 2023). Several answers show that smaller businesses do not possess expertise in this field and therefore do not know what to do and how to prepare (DSIT, 2023).

1.2 Research purpose

The purpose of this thesis is to highlight the importance of cybersecurity for small and medium sized enterprises (SME). As we are heading towards more and more digitalized future, SMEs should seek to protect themselves from the cyber threats by gathering knowledge and putting in place formal processes (DSIT, 2023).

I want to improve the knowledge about risk and cybersecurity for people who aren't necessarily competent in that field and the way I want to do that in is by presenting these two

main topics in a simple way that will be as easy to understand as possible. To do this, the final product will be a framework focusing on how to deal with cyber threats in small and medium sized enterprises that do not have designated in-house IT personnel. The development of this framework is based on the latest thinking in risk science and an internationally recognized standard within the information security domain. The ISO 27001, Information security, cybersecurity and privacy protection – Information security management systems – Requirements is an international standard for establishing, implementing, maintaining, and continually improving an information security management system (Standard Norge, 2022, p. v). In addition to ISO 27001 I will also be using the latest theories, models, and principles in risk science to develop a tailor-made process which handles cybersecurity in the SME segment. This thesis will focus on what SMEs should be responsible for so that they can continue to operate in a safe manner. The thesis will cover the simple things such as using unique and strong passwords, frequent password change and authentication processes, updated security software and operating systems, but also how to assess these risks by using a risk science approach.

ISO 27001, as an international standard for information security management is very detailed and even though it is meant for organizations of all sizes, it still demands a lot of work from organizations to be applied in its entirety (Standard Norge, 2022, p. 1). An SME most of the time will not have the possibility to assign as many resources to follow such practices as a large organization would. Based on this, the thesis will also attempt to narrow down what are the most important practices to apply and how these practices should be prioritized considering limited resources SMEs often have.

1.3 Research question

My research question is:

What is the significance of cyber threats towards SMEs, how the cyber threats are perceived and how should SMEs manage the cybersecurity risks?

1.4 Thesis disposition

In chapter 1.0 Introduction, I will be explaining what the background of this thesis is, what it's research purpose is and will also state the research question this thesis aims to answer. The introductory section will also explain a central term of the thesis which is SME (small and medium-sized enterprises).

Chapter 2.0 Method will be focused on covering quantitative and qualitative research methods, and literature review. This chapter will also explain what research method I will be using, addressing the reasons for my choice and what challenges this research method will face.

Chapter 3.0 Background theory and data will firstly address how the term "risk" as a concept is defined in risk science and why it is defined in such a way, the terms closely related to risk such as vulnerability, resilience, uncertainty, and strength of knowledge will also be covered. Further, I will explain risk perception and risk assessment, which are some of the most important topics in risk science, additionally, this section will cover the ISO 27001, a standard that focuses on information security management systems. Furthermore, the thesis will focus on general theory about what cybersecurity is, types of cyberattacks, how they occur, and whether information security and cybersecurity can be used interchangeably. This part will also cover cyberattack trends, cybercrime in Norway, and what role Norwegian authorities play in cases that revolve around cyberattacks.

Chapter 4.0 Findings and Discussion will trough information gathered in previous section present and discuss findings by presenting some of the risk events related to cybersecurity, and by answering the questions of why SMEs should protect themselves from cybersecurity risks and how SMEs perceive cybersecurity risks. To end this section, the thesis will present a framework which aims to help SMEs establish cybersecurity practices in their organizations.

And the thesis ends with chapter 5.0 Conclusion where the thesis is summed up with some reflections and suggestions for future research.

1.5 Small and medium-sized enterprise

When using the term "SME" there is no universal and globally accepted definition (Madani, 2018, p. 105). To construct a universal definition for SMEs appears to be a very difficult task since these companies vary in size, economy, branches, sectors etc. depending on where in the world they are located in (Madani, 2018, p. 106).

There still exists a trend in how an SME is identified, majority of public authorities use the number of employees as the main criteria which decides whether a company is or isn't an SME but may include several more criteria such as the ownership structure, the income and the sector of economic activity (Madani, 2018, p. 106).

In this thesis, when referring to an SME I will be using the Norwegian definition of an SME. A definition of an SME in Norway uses only one criterion which is the number of employees,

thus a company is considered an SME when number of employees is 100 or less, a company with 1-20 employees is considered small while a company with 21-100 employees is considered as medium-sized company (NHO, n.d.). In Norway, SMEs account for more than 99% of all companies in Norway, these SMEs stand for 44% of the Norwegian annual value creation which makes for almost 700 billion Norwegian kroners (NHO, n.d.). In 2012, there was around 480 000 SMEs in Norway, there is also great variation in number of employees depending on which branch the SME operates in (Nærings og handelsdepartementet, 2012, p. 13). Almost 60% of all the SMEs in Norway had no employees, but when looking at specific branches such as agriculture, forestry, and fishing almost 90% of the companies had no employees, while only 1 in 4 companies in finance and insurance had no employees (Nærings og handelsdepartementet, 2012, p.13).

2.0 Method

2.1 Quantitative and qualitative methods

In context of performing research such as this one, a method is a tool we use when we want to research something (Dalland, 2017, p. 52). Method helps us to gather data/information we need for our research (Dalland, 2017, p. 52). The research methods are mainly divided into quantitative and qualitative methods (Dalland, 2017, p. 52). The benefit of a quantitative research method is that it gives us data in form of measurable units, numbers give us an opportunity to perform calculations of for example, average income of a certain population (Dalland, 2017, p. 52). The qualitative research methods aim to capture an opinion or an experience which is impossible to present by using numbers and measurements (Dalland, 2017, p. 52). Both of these methods contribute to research in their own way, in an effort to improve our understanding about society we live in, and how individuals, groups and institutions act and interact with each other (Dalland, 2017, p. 52).

In quantitative scientific research, we start off with a research question which indicates who we want to know something about and what we want to know about them (Tufte, 2014, p. 71). To highlight the research question, we need information (data) that measure the phenomena we are interested in (Tufte, 2014, p. 71). We can gather our own data (primary data) or use the data gathered in by someone else (secondary data) (Tufte, 2014, p. 71). Some of the most common characteristics of a quantitative research is that it is systematic, meaning that usually surveys are given with fixed answers, data collection is done without direct contact with the field being studied, the presentation of findings aims to provide explanations, also by using quantitative research method, the researcher looks at the phenomena from the "outside" and strives to be neutral in their research as much as possible (Dalland, 2017, p. 53).

Traditionally, qualitative methods have been tied to research that consists of close contact between the researcher and the people in the field by participatory observation and interview (Thagaard, 2018, p. 11). In the later years, studies about websites and digital communication have become an important source for qualitative analyses (Thagaard, 2018, p. 11). By having a qualitative approach, we also accomplish an understating of social phenomena because of the connections we establish during the time we spend in a certain field (Thagaard, 2018, p. 11). Also, interviews contribute to a development of how people experience and reflect over their own situation, as well as how people relate to each other (Thagaard, 2018, p. 11). The qualitative methods are mostly divided into 5 categories which are, observation, interview, analysis of existing texts and visual forms of expression, analysis of audio and video

recordings, and internet which represents different possibilities for qualitative research, this type of research method is applied when we take interviews via internet, the online interviewing also gives us access to people across large geographical areas (Thagaard, 2018, p. 12). Common characteristics of a qualitative research are going in-depth and an effort to present lots of information from a small sized survey unit, this method is also flexible as the interviews done are characterized by flexibility without fixed answers, by doing so, qualitative method tends to be much closer to the field that is being studied, unlike the quantitative method (Dalland, 2017, p. 53).

Different questions and problems can be tackled by different methods which means that a researcher has to make a choice on which method they are using, but also reflect on why that method is the most viable method to use (Dalland, 2017, p. 54). Such choice requires some consideration about what is the ideal approach and what is practically achievable (Dalland, 2017, p. 54). Both ethical assessment and what methods the researcher can perform successfully are important for the method choices, as well as what is economically and time wise realizable (Dalland, 2017, p. 54).

When research is completed, researcher has to discuss the method again and this involves self-criticism, researcher should then consider how the chosen method has worked and whether the method choice was good enough to come to a good answer to the research question (Dalland, 2017, p. 55). A researcher should also review the results openly, in a case where it appears that another method would be more suitable for the research or that the knowledge used was uncertain, the researcher should clearly state this, these cases also open new doors for another research and can be of help to a next person who decides to research the same topic (Dalland, 2017, p. 55).

2.2 Literature review

Literature review is a process in which we analyze existing literature against a topic, research area, theme, or discipline by identifying relevant theories, key constructs, empirical methods, contexts and remaining research gaps so that our analysis can provide future research with valuable information based on those gaps (Paul & Criado, 2020, p. 6). This is then a theoretical thesis that builds upon data and materials taken out from books and other written sources (Pettersen, 2008, p. 121). To perform good literature review, it is necessary to be critical, which helps the researcher in developing a thorough understanding of previous work that is related to the research question and objectives (Saunders et al., 2019, p. 116). In this type of method, there is no pre-defined structure, but it is normal to start at a more general

level before narrowing it down to the specific research question (Saunders et al., 2019, p. 116). The literature search involves multiple channels which consist of searching by using online databases and search engines, following references in the articles that have already been read and scanning, and browsing books and journals in the university library (Saunders et al., 2019, p. 116). The literature obtained must be evaluated for its relevance and value it brings to answer the research question and objectives (Saunders et al., 2019, p. 116).

2.3 Method choice

For this thesis, I will be having a qualitative approach anchored on scientific literature. My main source of information about risk science and cybersecurity are the books from the risk analysis and governances master's curriculum, online and physical library of University in Stavanger, as well as the search engine Google Scholar which offers wide range of scientific articles, books, and journals. By using these sources for my background theory I was able to ensure credibility and quality of the information provided in this research, in addition I have made sure that all of the journals, articles, and books are relevant for my research question (Thagaard, 2018, p. 119).

Cyberattacks seem to still be a taboo topic in the business world since these cases have an ability to cause great reputational damage, therefore these cases don't often go public, and if they do, companies will rarely give a statement to the media on how and what exactly happened. Because of this, in order to give some examples of a cyberattack on a SME I had to look through different Norwegian news outlets which have interviewed companies that have experienced a cyberattack. Even though I want to limit this thesis to Norway only, I had to gather the existing quantitative data from surveys performed by other companies (secondary data) and these are most of the time performed on a bigger and wider scale, but even though the research question of those researches is not the same as mine, it is still possible, when critically looking at that data to gather information relevant for my research.

As this has proved to be a challenging topic to gather information about, especially when facing the challenge of not having a good network in the business world, when not using the Google Scholar search engine or scientific papers from university's physical and online libraries I made sure to gather data from sources such as Cyber Security Consultants, Norwegian Business and Industry Security Council, and the Norwegian National Security Authority.

At the time of choosing my research question I have assumed that the cybersecurity in SME segment was not taken as seriously as it should be. This assumption of mine can be seen as preconception, which is something a researcher cannot free themselves from, but at the same time, a conception can gradually be modified as I gather more knowledge about a certain topic over time (Fangen, 2010, p. 47). It is also impossible to dive into a topic without having some form of opinion or a view on it from before, but by acquiring some knowledge on the topic I have researched and by being open-minded I could approach the field in a more appropriate way (Fangen, 2010, p. 47). Even though I have had certain expectations of what the results of my research will be, I had to not allow myself to be influenced by them to a degree in which it would affect my research negatively, but instead approach this research as objectively as possible (Fangen, 2010, p. 50).

To further strengthen the reliability of my research, whenever using someone else's work I have made sure to appropriately reference the author/s, by doing so a reader is able to find the original source of information through the reference list (Bailey, 2003, p. 73).

3.0 Background theory and data

3.1 Risk concept

When going for a bicycle ride a person is performing an activity (A), this activity will lead to a consequence (C) which can be both desirable and undesirable, a desirable C of performing this A would be that this person performs this activity as intended (travels from point A to point B with no issues), while undesirable consequence would be that the person gets injured or loses their life. This is an example that brings us to the first definition of risk proposed by Aven & Thekdi (2022, p. 10), "the potential for undesirable consequences". In this definition, the consequences considered are only those that are undesirable (Aven & Thekdi, 2022, p. 10). The word "potential" is mainly focused on consequences, but also points at uncertainties (U), which in this example means that the result of the activity may be an injury or a fatality, but we do not know until the activity is realized (Aven & Thekdi, 2022, p. 10).

This brings us to the second definition of risk, "the consequences of the activity and associated uncertainties" (Aven & Thekdi, 2022, p. 11). In this definition, both uncertainties and consequences are incorporated, these are also considered as two main components in the risk concept (Aven & Thekdi, 2022, p. 11). If we again look at the example from earlier, but use the latter definition of risk we are encouraged to look at both types of consequences, a person riding a bicycle is facing a risk which has undesirable consequences (injury, death, damaged bicycle), but on the other had it also has desirable consequences which is that the person makes the ride from point A to point B with no issues, still there are uncertainties since the activity has not been realized yet (Aven & Thekdi, 2022, p. 11).

Often, we relate consequences to a reference value (r), commonly this relates to current state, planned level or meeting an objective (Aven & Thekdi, 2022, p. 11). This is described in the third definition as "the deviation D from a 'reference value' r, and associated uncertainties" (Aven & Thekdi, 2022, p. 11). Say that reference value is planned production level, then deviation D is equal consequences C (actual production level) minus reference value (r), an easier illustration of this is: D=C-r (Aven & Thekdi, 2022, p. 11).

When dealing with risk it is important to define what the activity A represents, although sometimes an activity would be easily understood, other times it would be required to specify what the activity encompasses, a very usual example of this is including a time frame for example when discussing an activity with some type of risk (Aven & Thekdi, 2022, p. 12). To illustrate this we can use the example of riding a bicycle and risks related to this activity but give this activity a time frame for next 2 years.

3.1.1 Vulnerability and resilience

Vulnerability and resilience are some of the most important concepts related to risk (Aven & Thekdi, 2022, p. 16). The vulnerability concept in risk science is interpreted as "the potential for undesirable consequences given an event", to explain this we can think of a system in a technical structure, we say that a system is vulnerable if an error in one part of the system leads to the failure of the entire system (Aven & Thekdi, 2022, p. 18).

When it comes to the resilience, it is defined as "the ability to quickly return to the normal state given an event" and "the ability of the system to sustain or restore its basic functionality following an event" (Aven & Thekdi, 2022, p. 18). Again, we can use a system in a technical structure as an example, time is a very common element which is used to determine how resilient a system is, thus if a system after a failure recovers to a normal state quickly it is resilient, but if it doesn't, we can say that the system is not very resilient (Aven & Thekdi, 2022, p. 18).

3.1.2 Strength of Knowledge

When discussing any type of risk it is important to have knowledge about those risks to manage them in a good way and also this knowledge should be evaluated (Aven & Thekdi, 2022, p. 35). When gathering knowledge about risks it is generally founded on data, information, modeling, testing, argumentation and often, the knowledge can be formulated as assumptions (Aven & Thekdi, 2022, p. 36). Knowledge can also be split into generic knowledge and specific knowledge, say we are interested in risks about operating an already existing restaurant, then generic knowledge would be all of the knowledge related to food and drink industry, while specific knowledge would be related to the knowledge that is aimed at the specifically that one restaurant (Aven & Thekdi, 2022, p. 36). Knowledge as a concept is very similar to the concept of evidence used in courts (Aven & Thekdi, 2022, p. 36).

When all the knowledge is gathered we need to evaluate it and this evaluation is referred to as strength of knowledge (SoK) (Aven & Thekdi, 2022, p. 35). To do this, we use a scale such as: weak knowledge, medium strong knowledge, and strong knowledge (Aven & Thekdi, 2022, p. 35). For knowledge to be judged as strong we need to have a lot of relevant data supporting the probability judgments or a strong understanding of the phenomena studied, on the other hand, if we do not have such data, the strength of knowledge is considered weak (Aven & Thekdi, 2022, p. 35).

Some of the most common topics to consider when judging the strength of knowledge are the amount and relevancy of data/information, the reasonability of the assumptions, the degree of

agreement among experts, the degree to which the phenomena involved are understood and accurate models exist etc. (Aven & Thekdi, 2022, p. 35).

3.1.3 Uncertainties

Tied to risk, there are uncertainties which need to be addressed (Aven & Thekdi, 2020, p. 7). The uncertainty in risk science can be explained as not knowing the true value of a quantity or the future consequences of an activity, or incomplete knowledge about a hypothesis, a quantity, or the occurrence of an event (Aven & Thekdi, 2022, p. 305).

To assign uncertainties to consequences, there are two ways we can go about it (Aven & Thekdi, 2020, p. 11). Firstly, we attempt to obtain a characterization of the uncertainties which is as much as possible objective or intersubjective, and reflects the evidence available (Aven & Thekdi, 2020, p. 11). Secondly, we provide a subjective characterization of the uncertainties by the risk analysts, reflecting their knowledge and judgements which ofte, are on the basis of input from other experts (Aven & Thekdi, 2020, p. 11).

To characterize uncertainties of specified consequences (C'), we need three elements (Aven & Thekdi, 2020, p. 12). The first element is knowledge-based probabilities, which also can be referred to as subjective probabilities. The second element is judgement of strength of knowledge which supports these probabilities (Aven & Thekdi, 2020, p. 12). The third and final element is the knowledge that probability and strength of knowledge are based on (Aven & Thekdi, 2020, p. 12). Also, it is important to thoroughly examine the knowledge so that potential surprises can be revealed (Aven & Thekdi, 2020, p. 12). So, to measure or describe the uncertainties it is recommended to use the combination of probability and a strength of knowledge judgement (P, SoK) (Aven & Thekdi, 2020, p. 12).

3.2 Risk perception

Human behavior is primarily driven by perception and not by what is understood as facts by risk analysts and scientists (Renn, 2008, p. 93). The perceptions are formed by common-sense reasoning, personal experience, social communication, and cultural traditions, humans also link certain expectations, ideas, hopes, fears, and emotions with activities or events that have uncertain consequences (Renn, 2008, p. 93).

To assess information, humans tend to follow relatively consistent patterns of creating images of risks and evaluating them, which are related to certain evolutionary bases of coping with dangerous situations (Renn, 2008, p. 93). When a human faces a threat, they react with four basic strategies: fight, flight, play dead, and, if appropriate, experiment (Renn, 2008, p. 93).

Over the course of cultural evolution, basic patterns of perception were increasingly enriched with cultural patterns which can be described by so-called qualitative evaluation characteristics (Renn, 2008, p. 93).

The qualitative evaluation characteristics go beyond the two classical factors of risk assessment on which risk is usually judged: probability and degree of possible harm (Renn, 2008, p. 94). In this case, psychologists differentiate between two classes of qualitative perception patterns: risk-related patterns based on the properties of the source of risk, and situation-related patterns based on the idiosyncrasies of the risky situation (Renn, 2008, p. 94). An example of risk-related pattern can be people riding in a car thinking that in case of a traffic accident they would come out with no injuries, but if they were sitting in an airplane and if something was to happen, there is no getting away (Renn, 2008, 94). This feeling of apprehension does not lessen even if they know that statistically, more people die in car accidents than in airplane crashes (Renn, 2008, p. 94).

Situation-related patterns of perception include aspects such as "voluntariness" and the ability to exercise personal control, which means that if someone is convinced they are in control of risk, they perceive it as less serious (Renn, 2008, p. 94). This type of thinking is very common when it comes to eating habits, specifically when people believe they can easily do without consuming sweets, alcohol or other types of food generally considered unhealthy only if they wanted to (Renn, 2008, p. 94). But, people show special concern to risks that they believe are not properly controlled by public authorities, such as genetically modified organisms also referred to as GMO (Renn, 2008, p. 94).

People also tend to stigmatize risk sources that are associated with specific dreadful associations, an example of stigma is a reaction to products that are deemed to be carcinogenic, even though there is often limited or hardly any scientific evidence to support this claim (Renn, 2008, p. 94). Just a suspicion that a specific substance could cause cancer is often enough to generate fear and demand for strict regulatory action (Renn, 2008, p. 95). Stigmatization often leads to public outrage and regulatory response feed into the process which can also be described as social amplification of risk (Renn, 2008, p. 95). Mass media reporting often results in public's perception of risk becoming amplified and people tend to have difficulties in interpreting low probabilities when making decisions, also people sometimes tend to not want to know data on the likelihood of an event occurring (Renn, 2008, p. 95).

There are also certain patterns people use to draw inferences about probabilities and risks, one of those is availability bias which can be explained as a tendency to overestimate probability of a certain event if a individual is able to recognize the risk fast and easy, an example of this is if a person has known someone who was struck by lightning they would perceive the probability of them getting struck much higher than someone who hasn't (Renn, 2008, p. 95).

Another such pattern is called anchoring effect which refers to risks that provoke associations with known events which increases likelihood of probability being overestimated (Renn, 2008, p. 95). If a risk source has constant and similar losses it is more likely that the impact of average losses will be underestimated, example of this is road traffic accidents, while these are not deemed acceptable they are still in a way, passively accepted, this pattern is called distribution of risks over time, if annual number of traffic accidents was to occur at the same time and not distributed over a year the rejection would be a lot higher, people also tend to prefer loss distribution over individual disasters (Renn, 2008, p. 95).

The last pattern we will mention is assessment bias in which the greater the uncertainty of loss expectation is, the more likely the average loss assessment will be in the region of the median of all known loss expectations, also loss expectations in low risks are often overestimated while objectively high risks are often underestimated (Renn, 2008, p. 95).

Besides psychological elements that influence people's risk perception, there are also social and cultural drivers of risk perception (Renn, 2008, p. 98). One of the most prominent social and cultural factors is value commitments, which are mental constructs that allow individuals or groups to assess a set of objects and/or state of affairs as good or bad (Renn, 2008, p. 119). Some of these values are traditional values (patriotism, regional or ethnic identity, social status and family stability), work ethics (diligence, punctuality, efficiency, discipline, and deferred gratification), hedonistic values (consumption, enjoyment, fun and immediate gratification), and post-materialistic values (harmony, social responsibility, environmental quality, decentralization and quality of life) (Renn, 2008, p. 120). These values do influence risk perception, but not in a very considerate amount, the values are more of a selection and attention filters and add emotional color to processing and weighing of conflicting information on risks (Renn, 2008, p. 121).

Another social and cultural driver of risk perception is referred to as institutional trust and credibility, which comes from the belief that most information about certain risk is not learned through personal experience, but through "second-hand" learning and people are more

dependent on relying on the credibility and sincerity of those from who they receive information about risk form (Renn, 2008, p. 123). The components of "trust" in question are perceived competence, objectivity, fairness, consistency, sincerity, faith, and empathy, the lack of one component can often be compensated with another (Renn, 2008, p. 124).

The influence of media is also a driver of risk perception since a lot of people gather information about certain risks from media which in risk science is referred to as "intermediary sources" (Renn, 2008, p. 127). The two main challenges of media transmitting information are questions of whether the media is creating new messages or are they reflecting existing messages, and are journalists biased in their coverage in regard to their own social convictions and external pressures (Renn, 2008, p. 127).

To get a better picture of how risk perception is formed we can look at the structured framework that provides an integrative and systematic perspective on risk perception developed by Renn and Rohrmann in 2000 (Renn, 2008, p. 141). This framework points at four distinct context levels: heuristics of information processing, cognitive-affective factors, socio-political institutions, and cultural background (Renn, 2008, p. 141). Each of these levels are also divided into two subsections: collective and personal manifestations of risk perception (Renn, 2008, p. 142).

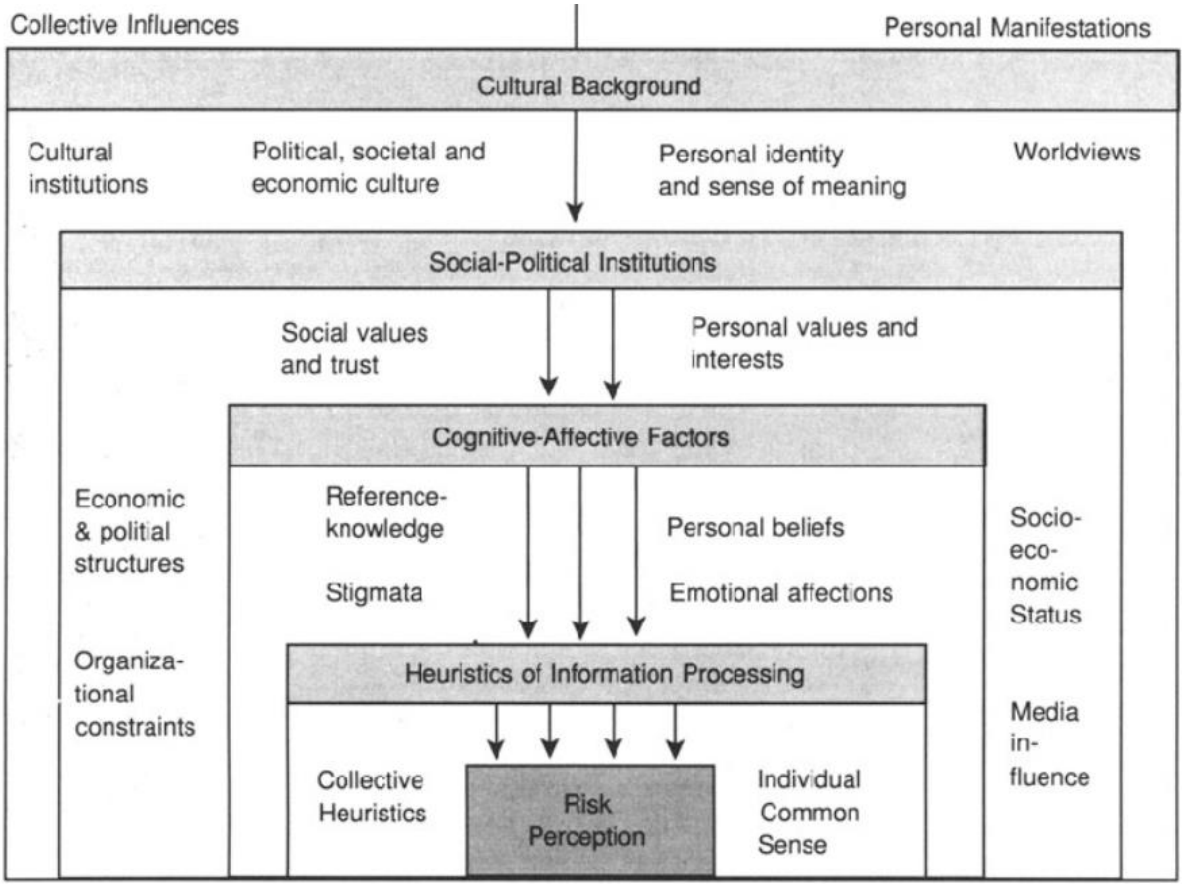


Figure 1 Four context levels of risk perception (Renn, 2008, p. 141)

These four levels of influence help us gain better and more accurate understanding of risk perception. This framework demonstrates us how individual and social factors shape risk perception, as well as it shows how risk is a multidimensional concept and not a simple combination of probabilities and consequences (Renn, 2008, p. 145). Still, this does not mean that professional risk assessment isn't important for people's perception since its one of many elements that shape the attitude towards risks and risks' acceptability judgements (Renn, 2008, p. 145). A good way to look at risk perception is to understand that risk perception demonstrates what matters to people, and in democratic societies the people's concerns should be the guiding principle for collective action (Renn, 2008, p. 146).

3.3 Risk Assessment

Risk assessment is a process in which we aim to improve our understanding of the risks considered and by doing so we support the decision-makers when deciding what actions to take, the key elements of a risk assessment are: 1. what can happen (‘go wrong’)?, 2. link risk events to consequences, 3. assess uncertainty, and 4. evaluate the risk, risk assessment process can also be divided into two main stages: risk analysis and risk evaluation (Aven & Thekdi, 2022, p. 61).

1. What can happen (‘go wrong’)?, is about leveraging past data, expert opinions, and trends so that the events that could cause negative or positive consequences can be identified (Aven & Thekdi, 2022, p. 61). By distinguishing between risk sources, threats, hazards, and opportunities, risk assessment teams gain an understanding of certain risk events (Aven & Thekdi, 2022, p. 61). It is impossible for risk assessment teams to list out every possible outcome but creating a preliminary list of outcomes is essential for a good risk assessment (Aven & Thekdi, 2022, p. 61).

2. Link risk events to consequences, refers to pin-pointing why and how potential risk events could result in negative or positive consequences, these consequences could also have a mix between good and bad aspects (Aven & Thekdi, 2022, p. 61).

3. Assess uncertainty, is an element in which we acknowledge uncertainty and use a characterization of uncertainty to frame an understanding of what can and will happen, we cover judgments about likelihood and strength of knowledge (Aven & Thekdi, 2022, p. 61).

4. Evaluate the risk, is about determining the significance of the risk and ranking the alternatives by using relevant criteria, then we are faced with management review and judgment which is a process of summarizing, interpreting and deliberating over the results of risk assessments, other assessments, and any other relevant issues in order to make a decision (Aven & Thekdi, 2022, p. 61). Management review and judgment is always needed as there are other aspects than the risk that are important for the decision-making, and also, risk assessment has it’s own limitations in capturing all aspects of risk (Aven & Thekdi, 2022, p. 61).

A good way to illustrate key features of risk analysis is to look at the bow-tie diagram (Aven & Thekdi, 2022, p. 76).

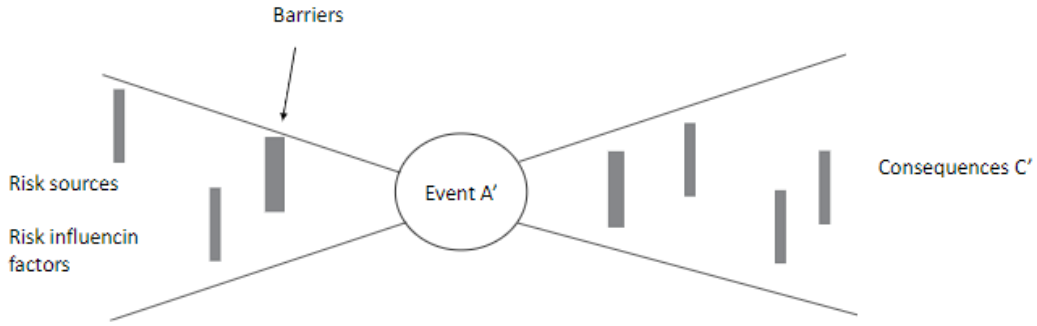


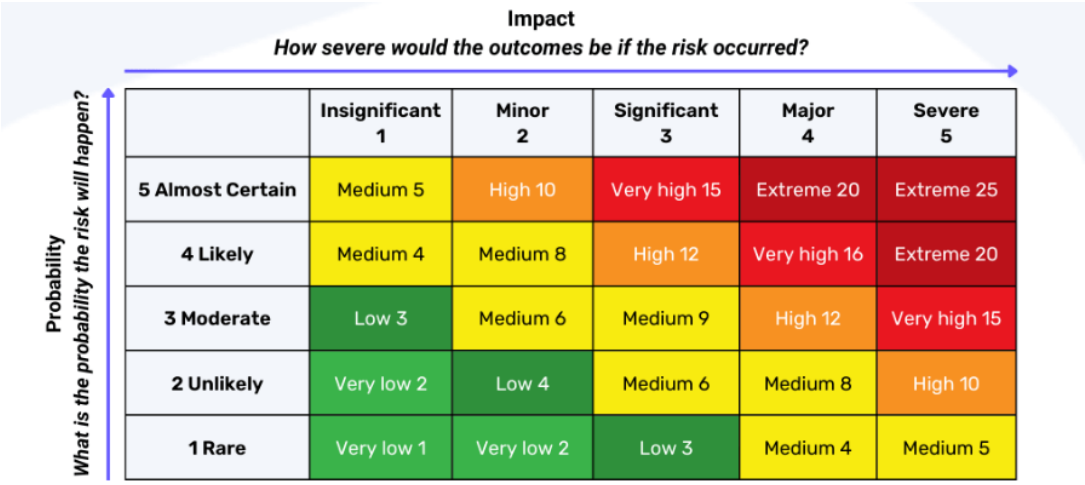
Figure 2 A schematic example of a bow-tie used in a risk analysis context (Aven & Thekdi, 2022, p. 76)

This diagram shows us the key features of a risk analysis, firstly we identify an event which can be a hazard, threat, or an opportunity, then we look into underlying events, risk sources, and risk influencing factors which can lead to the event happening (Aven & Thekdi, 2022, p. 76). Throughout this diagram we also see barriers, which serve to hinder an event from happening, but there are also barriers present in a case where the event does occur, the purpose of those is to reduce the effect of consequences as much as possible (Aven & Thekdi, 2022, p. 76).

3.4 Risk Matrix

A risk matrix is a tool, shaped like a table which is used in risk management to in a simple way illustrate risks by combining "probability", "likelihood", or "frequency" and "severity", "impact", or "consequences" (Cox Jr, 2008, p. 497). Risk matrices combining "frequency" and "severity" are popular and are used in various contexts such as terrorism risk analysis, highway construction project management, office building risk analysis, climate change risk management, and enterprise risk management (Cox Jr, 2008, p. 497). The risk matrices also help set priorities and guide resource allocations (Cox Jr, 2008, p. 498). What also makes risk matrices an attractive risk management tool to apply is that risks are color coded based on how serious they are (Cox Jr, 2008, p. 498). Most common colors to use are green, yellow, and red, where green stands for low risk, yellow stands for medium risk, and red stands for high risk (Cox Jr. 2008, p. 498). Another good thing about risk matrices is that it doesn't require any special expertise to construct, use, and socialize it within an organization (Cox Jr, 2008, p. 498).

An example of a standard 5x5 risk matrix can be seen below, rows represent the probability of a risk occurring and are labeled from 1 to 5 and described as 1= rare, 2= unlikely, 3= moderate, 4= likely, and 5= almost certain (Guevara, 2023). Columns represent the severity of the outcome if the risk event occurred and are also labeled from 1 to 5 and described as 1= insignificant, 2= minor, 3= significant, 4= major, and 5= severe (Guevara, 2023). Further classification of these "labels" are often defined by the needs of an organization (Guevara, 2023). For example, impact 1 which stands for insignificant can be defined as "won't cause injuries or illnesses", impact 2 which stands for minor can be defined as "can cause injuries or illnesses, only to a mild extent" and so on (Guevara, 2023).



	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very high 15
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

Figure 3 5x5 Risk Matrix Sample (Guevara, 2023)

Despite risk matrix being a frequently used method to illustrate risks, it doesn't address the uncertainties (Aven & Thekdi, 2022, p. 47). It doesn't take into account on what knowledge the consequence assessment is based on, or what the strength of the knowledge is (Aven & Thekdi, 2022, p. 49). To overcome this issue we can incorporate strength of knowledge judgments into the risk matrix (Aven & Thekdi, 2022, p. 47).

A way to do this can be seen in the figure below, this type of risk matrix is presented by Aven & Thekdi (2020).

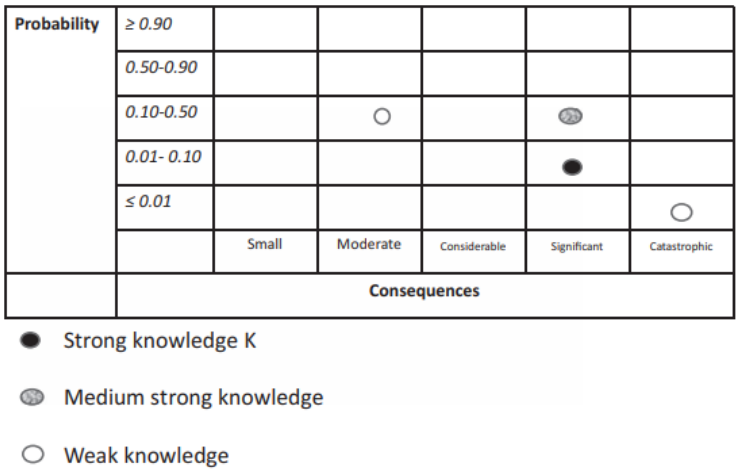


Figure 4 Example of extended risk matrix (Aven & Thekdi, 2020, p. 15)

When assessing risk it is important to recognize that strength of knowledge refers to the knowledge that analyst possesses, thus if the analyst has insufficient knowledge strength, it is important to classify a situation as "low strength of knowledge" (Aven & Thekdi, 2020, p. 132). This type of risk matrix serves as a decision-making tool that will allow the analyst to understand the importance and priorities of various risk events, therefore the information about judgement of strength of knowledge should be included for risk management activities (Aven & Thekdi, 2020, p. 132). In enterprise risk management process, the transparency is very important, in a case where analyst makes an assumption, especially in cases where expert knowledge is not available, information about that has to be disclosed (Aven & Thekdi, 2020, p. 132). Analysts should also act with integrity and are to disclose deficiencies in the analysis, since by doing so it also build credibility and invites others within organization to trust the process and the implementation (Aven & Thekdi, 2020, p. 133).

3.5 ISO 27001

The ISO 27001 is a document which provides requirements for establishing, implementing, maintaining and continually improving an information security management system (Standard Norge, 2022, p. v). An information security management system (ISMS) is meant to preserve confidentiality, integrity, and availability of information, and this is done by applying a risk management process (Standard Norge, 2022. p. v).

For an organization to claim conformity to the ISO 27001, it has to implement the requirements of 7 main clauses which are specified in clauses 4 to 10 (Standard Norge, 2022, p. 1).

Clause 4- Context of the organization

This clause consists of 4 key points which are understating the organization and its context, understating the needs and expectations of interested parties, determining the scope of ISMS and information security management system itself (Standard Norge, 2022, p. 1).

Clause 5- Leadership

The fifth clause sets focus on responsibilities of the top management and demands that top management shall demonstrate leadership and commitment with respect to the ISMS by for example ensuring that the ISMS achieves its intended outcomes, promoting continual improvement, ensuring that the resources needed for the ISMS are available, directing and supporting persons to contribute to the effectiveness of the ISMS, etc. (Standard Norge, 2022, p. 2). This clause also demands that top management shall establish an information security policy and that top management ensures that the responsibilities and authorities for roles relevant to information security are assigned and communicated within organization (Standard Norge, 2022, p. 3).

Clause 6- Planning

This clause is aimed at the planning phase of the ISMS, for this clause the organization shall consider issues and requirements and determine the risks and opportunities that need to be addressed so that organization can ensure that ISMS can achieve it's intended outcomes, prevent, or reduce undesired effects and achieve continual improvement (Standard Norge, 2022, p. 3). The organization should define and apply an information security risk assessment process that establishes and maintains information security risk criteria, ensures that repeated information security risk assessments produce consistent, valid, and comparable results, and that this process identifies, analyzes, and evaluates the information security risks, in addition, the organization should also define and apply an information security risk treatment process (Standard Norge, 2022, p. 4). Information security objectives are to be established together with a plan on how to achieve them, also if there is a need for changes in the ISMS, this is to be carried out in a planned manner (Standard Norge, 2022, p. 5).

Clause 7- Support

The support clause covers the topic of resources and demands that the organization determines and provides the resources needed for the establishment, implementation, maintenance, and continual improvement of the ISMS (Standard Norge, 2022, p. 6). This clause focuses on the topics such as competence where the organization should ensure they have the necessary competence present, awareness which means that people doing the work under the organization's control should be aware of the information security policy, their contribution to the effectiveness of the ISMS, and the implication of not conforming with the ISMS requirements (Standard Norge, 2022, p. 6). Communication is also a part of the support clause, here, the organization should determine what is to be communicated, when to communicate, with whom and how to communicate (Standard Norge, 2022, p. 6). And lastly, support clause also covers the topic of documented information, where it is specified what information is to be documented, the appropriate steps in creation and updating of information, and how the documented information is to be controlled (Standard Norge, 2022, p. 7).

Clause 8- Operation

This clause states that the organization should plan, implement, and control processes needed to meet requirements, and to implement the actions of establishing criteria for the processes and implement control of the processes in accordance with the criteria (Standard Norge, 2022, p. 7). The organization needs to also perform information security risk assessments at planned intervals or when significant changes are proposed to occur, also the organization will have to implement the information security risk treatment plan (Standard Norge, 2022, p. 8).

Clause 9- Performance evaluation

The organization is to determine what needs to be monitored and measured, the methods for monitoring, measurement, analysis, and evaluation, when the monitoring and measuring is to be performed, who will monitor and measure, when the results are to be analyzed and evaluated, and who should analyze and evaluate these results (Standard Norge, 2022, p. 8). Internal audits are to be conducted at planned intervals to provide information on whether ISMS conforms to the organization's own requirements and the requirements of ISO 27001, and also to check if the ISMS is effectively implemented and maintained (Standard Norge, 2022, p. 8). In addition, the organization is to plan, establish, implement and maintain an audit programme which includes frequency, methods, responsibilities, planning requirements and reporting (Standard Norge, 2022, p. 9).

The top management is also to review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness (Standard Norge, 2022, p. 9). This review is meant to include considerations such as feedback on the information security performance, feedback from interested parties, results of risk assessment and status of risk treatment plan, opportunities for continual improvement etc. (Standard Norge, 2022, p. 9). It is also necessary that the results of the management review include decisions related to continual improvement opportunities and any needs for changes to the ISMS (Standard Norge, 2022, p. 9).

Clause 10- Improvement

The organization is to continually improve the suitability, adequacy, and effectiveness of the ISMS (Standard Norge, 2022, p. 10). In the event that a nonconformity occurs, the organization is to react to it accordingly, evaluate the need for action to eliminate the causes of nonconformity so it doesn't reoccur or occur elsewhere, implement any action needed, review the effectiveness of any correction action taken, make changes to ISMS, and document the nature of the nonconformities, and the results of the corrective action (Standard Norge, 2022, p. 10).

3.6 Cybersecurity

Cybersecurity is a very broad term which at times can be difficult to define (Craigen et al., 2014, p. 13). The context in which we use this term will heavily influence what definition we settle with (Craigen et al., 2014, p. 13). But, even though there are many definitions, all of them revolve around three key elements which are referred to as CIA, confidentiality, integrity, and availability (Craigen et al., 2014, p. 13). Confidentiality is described as information or data of any organization should be maintained in a safe manner and unauthorized users should not be able to easily access it (Uma & Padmavathi, 2013, p. 392). Integrity refers to that during transmission of information or data, it should not be altered, and it has to reach its destination just as it has been sent from the source (Uma & Padmavathi, 2013, p. 392). Availability means that important information of an organization should be stored in such manner that it is available to the authorized users, and it should not be easily accessible by the unauthorized users (Uma & Padmavathi, 2013, p. 392).

Some of the well-established cybersecurity definitions are as follows:

"Cybersecurity involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access,

enforce authentication, enable encrypted communications, and on and on." (Amoroso, 2006, as cited in, Craigen et al., 2014, p. 14).

"Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption." (Lewis, 2006, p. 1).

"The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitations." (DHS, 2014, as cited in, Craigen et al., 2014, p. 15).

In today's world where pretty much, everything can be done online it is important that everyone has some kind of cybersecurity knowledge in the back of their head. By stating this, I am referring to the simple stuff like not clicking on whatever thing pops up on the screen or not typing in personal information in whatever web page a person comes across.

As the digital world evolves, information security and data privacy are permanently facing risks (Bendovschi, 2015, s. 24). Cyber criminals are continuously developing new ways and techniques to gain access to networks, programs, and data with a goal of compromising the confidentiality, integrity, and availability of information (Bendovschi, 2015, s. 25). Cyber criminals target not only individuals, but also, small, medium, and big businesses (Bendovschi, 2015, s. 25).

There are many ways in which an organization can be attacked by cyber criminals, some of the most common ones are: man in the middle, brute force attack, DDoS, malware, phishing, and social engineering (Bendovschi, 2015, s. 25).

Man in the middle

A cyberattack is considered as "man in the middle" when an attacker is between two communication ends, every message sent between the ends goes through the attacker before it reaches its target, when this happens, attacker is able to get their hands on sensitive information as well as alter the messages before they reach their destination (Bendovschi, 2015, s. 25).

Brute force attack

A brute force attack is when an attacker by repeated attempts to discover the correct key (password, encryption, etc.) gains access to protected information (Bendovschi, 2015, s. 25).

It is a trial-and-error process which is a simple and frequently used technique for gaining unauthorized access to individual accounts and organizations' systems and networks (Fortinet, n.d.). Even though this technique is an older cyberattack method, it still remains used and still is a popular technique among hackers (Fortinet, n.d.)

DDoS

DDoS (Distributed Denial of Service) is considered when an attacker floods the victim with internet traffic to the point where the system becomes inoperable and thus compromises the availability of data (Bendovschi, 2015, s. 25). This type of cyberattack is issued by using a internet connected network of compromised machines and other devices which have been affected by malware, which lets the attacker control them, this type of network is also called a botnet (Cloudflare, n.d.).

Malware

Malware is a term that describes various types of malicious software which are used by attackers to compromise the confidentiality, availability, and integrity of data, some of the most common types of these software are: viruses, worms, ransomware, trojans, spyware etc. (Bendovschi, 2015, s. 25). A malware usually has as an objective to let the attacker control an infected machine, send spam from the infected machine to unsuspecting targets, gain access to the infected user's local network and steal sensitive data (Palo Alto Networks, n.d.). A malware can spread in many different ways, as an email attachment, through file servers, through file sharing software and peer to peer file sharing etc. (Palo Alto Networks, n.d.).

Phishing

Phishing is a way to trick the unsuspecting victims by simulating a trustful source such as a website, typically a victim would type in personal information into these websites which then would be stolen by the attacker (Bendovschi, 2015, s. 25). For example, even though a certain system is safe, it can still be exploited by the users in a case where the victim receives an email by the attacker and is asked to change their password by using the link in the email which is controlled and monitored by the attacker (Khonji, et al., 2013, p. 2091).

Social engineering

Social engineering is a term used when referring to an attacker gaining unauthorized access to information through human interaction (Bendovschi, 2015, s. 25). This is a tactic where the victim is manipulated and deceived in order to trick the victim into giving out sensitive

information and making security mistakes (Carnegie Mellon University, n.d.). Trough social engineering, attacker aims to gain control over a computer system or to steal personal and financial information (Carnegie Mellon University, n.d.). Social engineering is carried out in multiple steps, victim is first investigated, attacker gains background information about the victim, then attacker impersonates someone the victim knows and by doing that gains victim's trust which in the end results in attacker gaining what they seek (Carnegie Mellon University, n.d.).

3.7 Information security

Just as in cybersecurity, there are also many ways to define information security (Von Solms & Van Niekerk, 2013, p. 97).

"Preservation of confidentiality, integrity and availability of information" is one way of how we can define information security (ISO/IEC 27002, 2005, as cited in Von Solms & Van Niekerk, 2013, p. 98).

Already, we can see overlap between this definition and the definitions of cybersecurity, the main overlap is the use of the characteristics: confidentiality, integrity, and availability of information (Von Solms & Van Niekerk, 2013, p. 97). These characteristics have always been important for the industry, but we need to add more accuracy, authenticity, utility, and possession to the definition, and that is what Whitman and Mattord (2009) have done in theirs (Von Solms & Van Niekerk, 2013, p. 98).

According to Whitman and Mattord (2009) information security is "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" (Whitman & Mattord, 2009, as cited in Von Solms & Van Niekerk, 2013, p. 98).

When discussing information security in context of the two definitions mentioned above, firstly it is important to note that it is a process and not a product or a technology, also, the use of computers and networks is evolving, therefore the process of securing these computers and networks also has to evolve, secondly in addition to the three main characteristics confidentiality, integrity, and availability, information security can include more characteristics (Von Solms & Van Niekerk, 2013, p. 98). The term information and communication technology (ICT) is used when referring to dealing with the protection of actual technology-based systems on which information is commonly stored and/or transmitted, therefore this term is different to the term information security (Von Solms & Van Niekerk, 2013, p. 97).

Currently, it is very common that terms cybersecurity and information security are used interchangeably since these overlap so much, but there are still some differences (Von Solms & Van Niekerk, 2013, p. 99). In a case where cybersecurity incident can be described in terms of the characteristics used to define information security, it is acceptable to use both terms synonymously (Von Solms & Van Niekerk, 2013, p. 99). For example, when cybersecurity incident also leads to a breach in the confidentiality, integrity or availability of information (Von Solms & Van Niekerk, 2013, p. 99). But, when a cybersecurity incident doesn't follow the formally defined scope of information security, then it is not acceptable to use both terms synonymously (Von Solms & Van Niekerk, 2013, p. 99). One such example is cyber bullying, which refers to causing embarrassment, invoking harassment and violence, and inflicting psychological harm which can lead to severe and negative impacts on those victimized (Von Solms & Van Niekerk, 2013, p. 99). Such cases of cybersecurity do not cause loss of confidentiality, integrity or availability of information which are the main characteristics when referring to information security (Von Solms & Van Niekerk, 2013, p. 99).

Security in general is about protection of assets from the various threats posed by certain inherent vulnerabilities, and all security processes usually deal with the selection and implementation of security controls which help to reduce the risk posed by these vulnerabilities (Von Solms & Van Niekerk, 2013, p. 100). In cybersecurity, the assets that need to be protected can range from an individual themselves, automated electronics in a household such as security systems, televisions or fridges to the interests of society at large, including critical national infrastructure (Von Solms & Van Niekerk, 2013, p. 100). In terms of ICT security, the assets that need protection are the underlying information technology infrastructures, while in terms of information security, these assets include all aspects of the information itself, including the protection of the underlying ICT assets, and then also assets that include information that is not stored or communicated directly using ICT (Von Solms & Van Niekerk, 2013, p. 100).

Even though terms cybersecurity and information security are often used interchangeably, the correct term to use depends on the assets in question (Von Solms & Van Niekerk, 2013, p. 101). Information security protects information from harm while cybersecurity protects not only the cyber space itself, but also protection of those that function in cyber space and any of their assets that can be reached via cyberspace (Von Solms & Van Niekerk, 2013, p. 101).

3.8 Cyberattack trends

Due to a business' size, cyber criminals would often assume that smaller businesses are easier targets (Rahmonbek, 2023). This assumption comes since naturally smaller businesses have weaker cybersecurity measures in place, are not financially prepared for an attack and often lack cyber insurance (Rahmonbek, 2023). Recently though, smaller businesses are becoming increasingly aware that strengthening their cybersecurity can minimize the risk of being targeted and potentially protect them from going out of business, since a successful cyberattack can have fatal consequences for a small business (Rahmonbek, 2023).

Looking at a few different surveys and studies we can see that in the last few years the percentage of small businesses being hit by cyber criminals has been increasing (Rahmonbek, 2023). Some of the reasons behind this are easier access and less security protections compared to the big enterprises (Rahmonbek, 2023). What also attracts cyber criminals to small businesses is the possibility to receive money from large number of companies, also the media attention and presence of law enforcement is far lesser than when dealing with a large enterprise (Rahmonbek, 2023).

In one of the studies, 61% SME's have experienced some kind of cyberattack although not all of these attacks have been successful, still it is worrying that the attacks are this common occurrence (Rahmonbek, 2023). The most common type of cyberattacks which are aimed at small businesses are malware, followed by data breaches, website hacking, DDoS attacks and ransomware (Rahmonbek, 2023). One study uncovered that 82% of ransomware attacks in 2021 were targeted at companies with less than 1000 employees and 37% at companies with less than 100 employees (Rahmonbek, 2023). The cause of this is believed to be the low risk of exposure in comparison to big businesses (Rahmonbek, 2023).

Malicious emails such as phishing, spam, and email malware are also most present at small businesses (Rahmonbek, 2023). In comparison to large enterprises, businesses with less than 100 employees experience 350% more social engineering attacks in which CEOs and CFOs are most popular targets, as well as executive assistants who own access to the accounts of high-level company members (Rahmonbek, 2023). In case of an attack, sensitive data such as credit card info, social security numbers, bank account info, phone numbers, and addresses can also be leaked and affect not only the business itself but also the customers and other associates of the business (Rahmonbek, 2023). Such leaks can lead to cases of identity theft, and other forms of privacy violations, in fact, a study found that 27% of small businesses with no cybersecurity protections collect customers' credit card information (Rahmonbek, 2023).

Attacking a couple of smaller businesses often equals the same amount of funds attackers would get from one large enterprise, so it makes sense why cyber criminals would attack smaller businesses, in addition, it takes less time and effort to succeed in attack on a business with weaker cybersecurity and generally it doesn't attract much unwanted attention (Rahmonbek, 2023). In a survey conducted by Momentive on behalf of CyberCatch, 75% of SMEs could not continue operating if they were hit with ransomware (Rahmonbek, 2023). Even if a business is able to pay the ransom, a reputation damage or potential lawsuit for leaking personal data like home address or credit card information can be the last drop that shuts down a business for good (Rahmonbek, 2023).

Besides all the negatives Covid-19 has caused, there can be seen an increase in cybersecurity preparedness among small businesses, mostly since a lot of employees worked from home which led to increased use of unsecured personal devices, but still there are many who think they are too small to be hit therefore having weak or none at all cybersecurity measures (Rahmonbek, 2023). There is also a sign of companies allocating budget for cybersecurity as they scale, around half of companies with less than 50 employees had no cybersecurity budget, 35% companies with 50-250 employees had no cybersecurity budget, and 18% of companies with over 250 employees did not have one (Rahmonbek, 2023).

3.9 Cybercrime in Norway

As a very digitalized country Norway is, companies in Norway are "bound" to experience some form of cyberattack. To create a picture of how and who is being targeted by cyber criminals in Norway as well as how these attacks are dealt with, we will be looking into the survey carried out by the Norwegian business and industry security council (Næringslivets Sikkerhetsråd).

This survey consists of 2500 respondents of which 89% are private sector and 94% are companies with 5 to 99 employees (Næringslivets Sikkerhetsråd, 2022, p. 8). The survey covers a large variety of industries which are spread evenly (Næringslivets Sikkerhetsråd, 2022, p. 9).

In this survey, 10% of 2500 companies have experienced attempted data breach/hacking and 9% have been targeted by phishing and other manipulative cyberattack techniques, these are also the most common undesired occurrences (Næringslivets Sikkerhetsråd, 2022, p. 15). The companies with 5-19 employees have on average experienced 1,8 undesirable situations, while companies with 20-99 employees have on average experienced 2,0 undesirable

situations (Næringslivets Sikkerhetsråd, 2022, p. 16). Of those who have been affected by ransomware (63), 26% have notified police and 25% have notified other authorities, 1% of those affected have paid to not be attacked again while no one has stated they have paid to remove the ransomware or paid so that their information doesn't go public (Næringslivets Sikkerhetsråd, 2022, p. 17).

When it comes to reasons for security breaches, it is mostly because of "coincidences or unfortunate events" (61%), 37% answered that security breach happened as a result from human error, and 28% answered it happened because of lack of security awareness amongst employees (Næringslivets Sikkerhetsråd, 2022, p. 21). The rest of the reasons are for example: insufficient processes (21%), lack of technical tools or competence to stop the threat (19%), existing processes not followed up (18%), use of home-office (11%), insufficient technical infrastructure (11%), conscious abuse of the systems (8%) etc. (Næringslivets Sikkerhetsråd, 2022, p. 21). Also, companies that have framework for information security have mostly noticed the security breach through routinely controls while companies that don't have information security framework have mostly noticed the security breach through pure coincidence or media reports (Næringslivets Sikkerhetsråd, 2022, p. 22).

After this type of events, it is very common that company's management gets involved and that the event is reported to the company's board, 19% have also answered that the event has led to economical loss (Næringslivets Sikkerhetsråd, 2022, p. 25). Companies with 20 or more employees have in larger degree invested into learning program for the employees and invested in security equipment (Næringslivets Sikkerhetsråd, 2022, p. 26).

PwC has also carried out a survey about cybercrime in Norway (PwC, 2022). When companies got asked what kind of events tied with cybercrime and other information security events they have experienced in the past 12 months, 81% answered phishing while other events like events caused by supplier, financial fraud targeted towards the company and unauthorized access to use of information, systems or network all lie at around 40% (PwC, 2022).

When it comes to consequences of cyberattacks, companies are most worried about critical systems not being available over long period of time, confidential information getting compromised or stolen, unauthorized access to personal data and company's brand and reputation being damaged (PwC, 2022). Also, 66% have own budgets for cyber and information security, naturally these companies are better prepared to handle the risks their

companies are facing, 66% are expecting that the budget for cyber and information security will increase in the next 12 months as well (PwC, 2022).

9 out of 10 answered that they themselves train their employees in general data protection regulation (GDPR), cybersecurity and privacy and with regular training, education, and testing a company becomes less vulnerable (PwC, 2022). This can be seen as a low investment with high yield as it stops many of the most common cyberattack types (PwC, 2022). The most used measures for awareness training associated with GDPR, cyber, and information security are E-learning with 73%, one-way communication with 64%, and classroom teaching with 36% (PwC, 2022).

Some of the results from the PwC's survey also point at the lack of competence and workforce in the field, this is a problem that gets highlighted since 46% respondents answered that they only to some degree have enough knowledge to protect themselves from cyber threats (PwC, 2022). PwC also writes that demand for security competence, combined with limited supply of specialists can be seen as national societal problem for years to come (PwC, 2022). The combination of lack of cybersecurity competence and rising threat of phishing is very threatening for businesses, but with simple measures the threat can be minimized by focusing on improving the cybersecurity competence (PwC, 2022).

In comparison with the year before, PwC could see that in general, companies have become more worried about the consequences of a cyberattack (PwC, 2022). More than half of the respondents are more worried about cyber threats in this year's survey than the year before (PwC, 2022). PwC is also predicting that in years to come, budget for cybersecurity will be more prioritized than it is now (PwC, 2022). The war in Ukraine has also had its effect on cybersecurity as 95% have answered that they are more worried for cyber threats because of the war (PwC, 2022). When asked whether they are planning to or have implemented new cybersecurity measures because of the conflict 57% have answered with "yes" (PwC, 2022).

Throughout the survey it can be seen that targeted cyberattacks have increased in comparison to the year prior (PwC, 2022). Targeted cyberattacks are seen as a dangerous threat because these are often designed for a specific target group which contributes to the attack being successful before it's uncovered (PwC, 2022). Also, targeted attacks indicate more motivated and potentially more competent threat actor (PwC, 2022).

This survey shows us that the focus on cybersecurity, digital competence, and safety culture in Norway is increasing (PwC, 2022). It is also important to note that the cyber threat is

continuously being developed so companies always need to be ahead of cyber criminals to make sure no serious harm is done to the company (PwC, 2022). Besides having employees with good digital safety competence, companies are also advised to regularly perform tests of their systems (PwC, 2022).

In 2016, a hair salon in Kongsberg, Norway has been a target of a cyberattack (Andreassen & Brendhagen, 2016). As soon as all computer screens in the salon went dark, the owner understood they are experiencing a cyberattack (Andreassen & Brendhagen, 2016). It all started with one employee that opened an attachment in an e-mail they received from who seemed to be their package supplier (Andreassen & Brendhagen, 2016). The attachment was a program that encrypted all of the data they had stored, and the computers got locked (Andreassen & Brendhagen, 2016). Shortly after the attack took place, the owner was contacted with instructions of how to get their files back, the hacker demanded 40 000,- NOK in bitcoin which was to be paid in 91 hours (Andreassen & Brendhagen, 2016). Even though the owner was advised by the national criminal investigation service (Kripos) to not pay the ransom, she still did it as she needed the data to keep the business running (Andreassen & Brendhagen, 2016). When NRK talked to Alex Backer, an IT consultant about this event, Backer said that people affected by a cyberattack rarely come out and speak about it as no one wants to admit to being hacked (Andreassen & Brendhagen, 2016). Very few such cases make it to police or the public in general, as people would rather pay the ransom (Andreassen & Brendhagen, 2016).

Another similar attack happened in Haugesund, when in April of 2022, owner came to work and was greeted with black screens on computers and all of the important business information missing (Mathisen, 2022). In this attack, a painting company that has been running for over a decade lost their customer register, offers, orders, time register and accounting (Mathisen, 2022). The company has lost millions (NOK) of revenue, employees quit, and the owner of the company has experienced some health issues as well (Mathisen, 2022). The attack was successful because the provider of cloud services got hit by a virus and the backup wasn’t stored properly, luckily company managed to survive and is still up and running (Mathisen, 2022). Today, the owner of the company advises people to make better contracts with their cybersecurity providers, and openly talks about his experience which he hopes will motivate others to be more careful and invest in cyber insurance (Mathisen, 2022).

3.10 Where does responsibility lie in case of a cyberattack?

The Norwegian National Security Authority (NSM) is Norwegian expert organ for information and object security, as well as the national specialist environment for ICT (information and communications technology), national cybersecurity center (NCSC) is established as a part of NSM (Nasjonalt cybersikkerhetssenter, n.d.).

NCSC is a arena for national and international cooperation in detecting, handling, analyzing, and counseling cases tied to digital security, the center includes partners from business, academia, military, and public sector which contributes actively in a mutual cooperation to make Norway more robust (Nasjonalt cybersikkerhetssenter, n.d.). NCSC is home to the national CERT*;NorCERT (Norwegian Computer Emergency Response Team) which handles severe computer attacks against critical infrastructure and information, their main activities are to respond to cyber threats and incidents 24/7, to detect data breaches in critical infrastructure across sectors via operating and organizing a national sensor network, and to perform reverse engineering, forensics, network analysis, and counterintelligence (Nasjonalt cybersikkerhetssenter, n.d.).

When a business is experiencing a cyberattack, normally there is need to act upon it as soon as possible, but at that time NCSC is not who businesses should rely on as NCSC themselves state on their webpage that they do not have capacity to assist all businesses, but they still want to be contacted so that they can get best possible picture of national situation, they also need to prioritize businesses of socially critical matter while other businesses are encouraged to contact their ICT provider or security provider (Nasjonalt cybersikkerhetssenter, n.d.). It is also stated that in a case where a business is exposed to attack, police should be contacted to decide whether the event should be reported (Nasjonalt cybersikkerhetssenter, n.d.).

When it comes to the role of police in cybersecurity cases, police want to be contacted and write a report on the case (Politiet, n.d.). They state that it is important to report all cybercrime and digital fraud so that they can evaluate whether the case will be investigated further (Politiet, n.d.). Police also emphasize that cybercrime is challenging to investigate and not all cases get resolved, but still mention the importance of making a report with all of the documentation that can be valuable for the cases in an effort to stop this type of criminal activity (Politiet, n.d.).

When a business is experiencing a cyberattack, it doesn't seem like Norwegian government is there to support them, but rather rely on their own cybersecurity measures that are either

established internally or outsourced (Hove et al., 2022). Businesses are also required by law to report the incidents, but it is not always easy to evaluate which incidents are serious enough that they need to be reported (Hove et al., 2022). If a business has outsourced their cybersecurity provider, they should clearly discuss the distribution of risk and responsibility for a cyberattack in advance as there is not enough time to discuss this as the attack is happening (Hove et al., 2022). A reason for successful cyberattack is often due to weaknesses situated at the company itself, for example an employee installing a harmful software or the outsourced cybersecurity provider not being able to prevent or avert the attack (Hove et al., 2022). If the responsibilities between the parties are established in advance it makes it simpler to pinpoint which party has made a mistake, although this evaluation will often be complex and sometimes the conclusion might be unclear (Hove et al., 2022).

4.0 Findings and discussion

4.1 Presenting the cybersecurity risks

To improve our understanding and make it easier to picture how probable and how impactful the cybersecurity risks are, in this section we will be presenting some risk events through an extended 5x5 risk matrix. The examples that will be presented will be based on organization that does not have any implemented processes in regard to combating cybersecurity risks.

Risks events will be color coded by green, yellow, and red. Green represents risks that are acceptable, yellow represents risks that are tolerable, and red represents risks that are unacceptable. If a risk is deemed acceptable (green) it means that the risk is under control and needs no special attention. Tolerable risks (yellow) are risks that need continuous attention so that they are kept under control, and if possible, seek to reduce the risk. Unacceptable risks (red) are risks that need immediate attention and should be of the highest priority in an organization.

In addition to subjective probability and consequence assessment, this risk matrix will also incorporate the judgements of strength of knowledge, so that uncertainties are addressed. The judgements of strength of knowledge will also be color coded, green= strong SoK, yellow= medium strong SoK, and red= weak SoK, and in the matrix these classifications will be represented as circles. Also, the severity of the risks will not be evaluated only by the combination of subjective probability and consequence, but also if a strength of knowledge is judged as weak or medium strong, the severity will be adjusted to one rank higher.

For example, if a risk event has subjective assessment of probability as 3 and assessment of consequence as 4, in the risk matrix it is placed on grid 12= tolerable, but if strength of knowledge is judged as weak or medium strong, the severity of risk is adjusted to be unacceptable, despite being in grid 12.

The ranks of subjective probability and consequences are classified as follows:

Subjective probability to occur:

Probability 1: Possible to occur, but probably never will

Probability 2: Not likely to occur

Probability 3: May occur

Probability 4: Expected to occur at some point

Probability 5: Will occur

Consequences:

Consequence 1: Negligible

Consequence 2: Minor

Consequence 3: Moderate

Consequence 4: Significant

Consequence 5: Severe

Now that we have established the classifications of subjective probability and consequence ranks and how these are affected by the judgement of strength of knowledge, we can take a look at what the risk matrix looks like.

	Consequence 1	Consequence 2	Consequence 3	Consequence 4	Consequence 5
Probability 5	5 Tolerable	10 Tolerable	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probability 4	4 Tolerable	8 Tolerable	12 Tolerable	16 Unacceptable	20 Unacceptable
Probability 3	3 Acceptable	6 Tolerable	9 Tolerable	12 Tolerable	15 Unacceptable
Probability 2	2 Acceptable	4 Acceptable	6 Tolerable	8 Tolerable	10 Tolerable
Probability 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Tolerable	5 Tolerable

Weak SoK

Medium strong SoK

Strong SoK

Figure 5 5x5 Risk matrix

4.1.1 Phishing

As we already have mentioned, phishing attack is a type of cyberattack in which attacker pretends to be trustful but has a goal of obtaining personal information such as usernames and passwords, credit card information, and other type of important data. This type of attack is commonly performed by attacker contacting the unsuspecting victim via e-mail.

To put this risk into a risk matrix we will be using the data we gathered. For subjective probability, we know that phishing attack is the most common type of cyberattack. And even though it is most common in both big businesses and SMEs, SMEs are still far more exposed to it since attacking SMEs usually doesn't attract attention from media and law enforcement, and also what plays a big part in this is that SMEs usually aren't good at protecting

themselves from cyberattacks, especially when we consider that most of the data breaches in Norway are due to coincidences, human error, and lack of security awareness. Based on this information we can say that the subjective probability assessment level of an SME to be hit by a successful phishing attack is 4 which is “expected to occur at some point”.

When it comes to consequences of phishing attacks, the very first consequence a business will encounter when hit by successful phishing attack is the economical loss. But it doesn’t stop there, very rarely will a business be affected economically only, but also reputational damage is most of the time present, which very quickly can be a “nail in the coffin” for a business, since customers would lose trust and stop using their services. And, if that wasn’t enough, a company could also face lawsuits if for example personal data was to be leaked. We can then say that the consequence assessment of a successful phishing attack is 5 “severe” since the company has no established routines on how to handle such type of attack.

We also need to make a judgement of our strength of knowledge. We have gathered our data and information from credible sources and experts which gives us good baseline, but since we are not experts in the cybersecurity field ourselves it would be reasonable to say that the judgement of knowledge is medium strong and not quite strong yet.

By combining our judgement of strength of knowledge, subjective probability and consequence assessment of this risk event and by plotting it into our risk matrix we end up with: probability 4 x consequence 5= 20 which is unacceptable risk. This means that the risk of phishing attack is something that needs to be prioritized and that risk reducing measures need to be implemented so that a company can still operate in a safe manner and “survive” being hit by a successful phishing attack. Below, you can see where on our risk matrix this risk event is placed.

Figure 6 Risk event: Phishing

4.1.2 Ransomware

All software that are designed to in some way damage or disrupt a computer system or a network fall under the term "malware". One of the most common types of malwares is ransomware. A ransomware encrypts victim's files with the main objective to extract money from the victim if they want to decrypt and get their files back (Gazet 2010, p. 77).

Just like phishing, ransomware is a very common cyberattack technique and a lot of attacks by ransomware are targeted towards SMEs. The reasoning for it is same as in phishing, doesn't attract attention from media and law enforcement, and usually bad cybersecurity measures in place. We also know that in some instances, companies would rather pay the ransom and hopefully solve the issue, rather than risk losing everything and taking a big hit which could put them out of business for good.

Since ransomware is spread to the victim in a similar way as phishing and also is a very common cyberattack technique, the subjective probability assessment of a successful ransomware attack will also be ranked as 4, "expected to occur at some point".

The consequences of this type of cyberattack are also very similar to the ones of phishing cyberattacks as it also revolves around the information. The main consequence of ransomware would be the economic loss. When hit by ransomware the company is faced with a dilemma of whether they want to pay the ransom or lose their files which most of the time would be crucial to have in order to keep operating a business. There is also a possibility where a company pays the ransom, but the attacker doesn't decrypt the files which then puts the company in an even worse position. When it comes to ransomware there is also the potential

for reputational damage and potential for lawsuits. For consequences of a ransomware infestation we can also say that it is a 5 “severe”, again, since the company has not established any measures to deal with such event.

In relation to strength of knowledge, our knowledge on this topic is same as in previous example, therefore we can judge it as medium strong.

With our judgment of strength of knowledge as medium strong, subjective probability assessment 4, and consequence assessment 5 we again end up with 5x4 which puts this risk event in grid 20, also “unacceptable risk” which calls for implementation of risk reducing measures and high spot on a list of priorities.

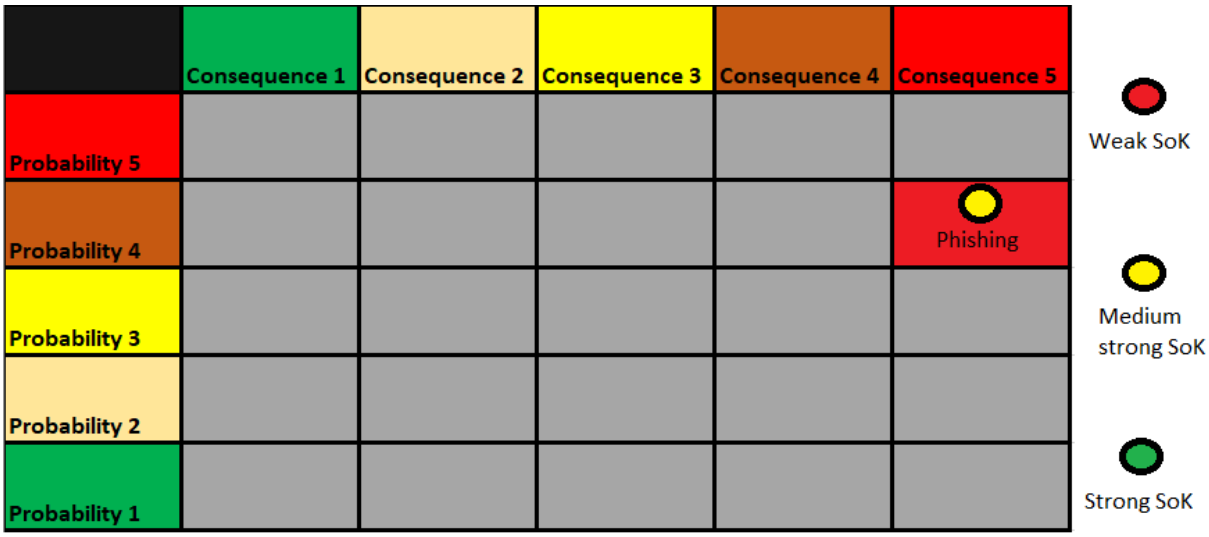


Figure 7 Risk event: Ransomware

4.2 Why should SMEs protect themselves from cyber threats?

During this research we have uncovered that main reasons for a cybersecurity breach have been human error, lack of security awareness amongst employees, insufficient processes, lack of technical tools or competence, use of home-office, insufficient technical infrastructure and more. To be able to properly deal with cybersecurity risks, or any other risks, the key thing to do is to assess the risks we are facing. We can do that by applying the process of risk assessment that was presented earlier in this thesis. By doing so, we can structure a bigger picture which would help us make right decisions in order to protect a business. First of all it can help a business to identify their vulnerabilities that are exploitable by people with bad intentions. It also guides a business towards good decisions when it comes to prioritizing resources as it uncovers areas that have the highest risks, thus a company can make better use of their limited resources. Important to remember is that risk assessment is not a one-time

operation, but rather a continuous process in which the security of a business is constantly improving. Risk assessment helps a business to create a plan in how to respond when an unwanted event occurs, increased understanding of potential risks leads to increased preparedness so that a business can minimize impact of an incident. While large enterprises usually have implemented a framework for information security and thus are better prepared against cyber threats, SMEs most of the time do not have same opportunities, whether it comes to the lack of funds or simply not having enough competence in that field, or they just don't perceive the cybersecurity risks as serious as they are. But, in the long run, by deciding to invest into cybersecurity, a business can save money in a sense that they avoid security breaches, legal problems, reputational damage and operation disruption. And the investment into the cybersecurity also builds trust with customers and other stakeholders, it also sends a message to the customers that they are a serious business. ISO 27001 also puts emphasis on how risk management is a process where it is important for organization to continually monitor and review their practices and from there on, seek improvement in what they do.

There is also an issue where the demand for competent IT specialists in Norway exceeds the supply to the point where it can be seen as a national societal problem for the future. This also can indicate that majority of SMEs probably do not possess required knowledge to deal with such risks.

Since a successful cyberattack in most cases is capable of shutting down an SME, we can say that SMEs are vulnerable to cyber risks. What is important then is to try to establish a system that will make a business resilient, also a system that can quickly recover to their original state after an undesirable event occurs, since many SMEs are bound to experience a successful cyberattack. The core element to building such system is to actively improve the knowledge about the cyber risks and transfer that knowledge onto people (employees) that function in that system, since effectively they are the first barrier a cyber criminal would be faced with and if a person is able to see that they are dealing with a potential cyberattack and responds to it accordingly, then we can say that the system is less vulnerable. But there will also be occasions where that barrier is breached and a successful cyberattack occurs, therefore it is important that a business knows how to resolve it, also knows how to minimize the impact, this is also referred to as a barrier even if it comes after the event has occurred.

Another reason for why SMEs should acknowledge their vulnerability and take ownership of their cybersecurity is because harsh reality is that they are alone in it. For example, if a burglary occurs in a convenience store there will be a lot of attention and support from law

enforcement, while same doesn't go for cyberattacks, even though it is also a criminal activity. Therefore, SMEs have to rely on their own capabilities and not hope that external parties such as police or other organizations will be able to come with some resolution or assistance. Even though different organizations do deal with cybercrime, usually their attention and resources may be focused on cases that they deem more important.

4.3 How do SMEs perceive cybersecurity risks?

By looking at the information we gathered, as the world experiences a rise in cyberattacks, we can see a positive trend where SMEs are more aware of dangers within cyber space. The rise in awareness about cyber threats can also be seen as a crucial step towards combating these dangers by SMEs implementing necessary measures to protect their sensitive data and critical business operations. By SMEs becoming more aware of the potential risks, we can also see a trend where some have started investing into their cybersecurity preparedness.

One factor that is very much present in the topic of cybersecurity tied to SMEs is that cyberattacks aren't really talked about and one doesn't really hear about them, even though data suggests that they are common occurrences. It is understandable though that businesses wouldn't want to share these events with the public as that would potentially cause more harm than good to them with reputational damage in mind.

On the other hand, if information about cyberattacks was more available, would it influence SMEs in a positive way where SMEs would start to look at these risks more seriously? Risk science suggests that having availability bias causes a tendency to overestimate probability of a certain event, but wouldn't it in this case having information about the cyber risks more available lead to having more accurate estimation of probability? At the same time, if this was to happen, we can not for sure know what effect it would create. Some may also argue that exposure to such information could lead to such amplification of cyber risks that it eventually generates so much fear which could cause people to avoid starting a business. Then we can see how this also could have a large negative impact in a country such as Norway where almost half of annual value creation is generated through SMEs.

4.4 Framework: Cybersecurity for SMEs

Introduction

Cybersecurity has steadily become one of the largest concerns for all companies no matter the size. As the technology develops, so does the risk and threat of cybercrime. In spite of size, SMEs are a frequent target of cyber criminals which are seeking to exploit their vulnerabilities and extract valuable information.

The aim of this framework is to address the challenges related to cybersecurity that SMEs face and help such businesses protect themselves. This framework will also be designed in such way that it provides a simplified approach to cybersecurity and will take into account that SMEs do not operate on equal footing such as large enterprises in terms of limited resources, expertise etc. Therefore, consider this framework as a tailor-made process that is effective and feasible to implement regardless of size and resources.

Additionally, the framework is a product inspired by the ISO 27001 and the newest thinking in risk science. It combines the best and simplest to apply practices of ISO 27001 together with latest findings risk science has to offer in an effort to provide a complete and up-to-date approach to cybersecurity.

By implementing this framework an SME will strengthen their defenses, reduce the risk of cyberattacks, and build a less vulnerable and resilient business environment.

Objective

The objective of this framework is to provide a simple, easy to understand and apply process which can help an SME to identify, manage, reduce, and monitor the cybersecurity risks they are facing. A successful implementation of this framework is when a SME manages to overturn all their unacceptable risks to tolerable and acceptable risks.

Key components

The key components of this framework are risk assessment, leadership, and employee awareness and training.

Risk assessment- This is a step where organization should identify potential risk events that could occur together with an outcome, even though it is impossible to list out every possible outcome it still gives the organization a good idea of possible undesirable situations. It is also desirable to research relevant data, expert opinions, and recent trends as this can often

improve the understanding of different risk events. Also, after the knowledge has been acquired, link events to possible consequences and construct a risk matrix which also incorporates judgments about strength of knowledge. Evaluate the weight of risk by assessing criteria such as subjective probability, impact, and strength of knowledge as this can help in visualizing the risk events so that the better idea of organization's exposure to risks is established. This evaluation can also help the organization with prioritization of risks.

Leadership- In a process such as this, it is very important that the top management serves as an example for the organization. The top management is to demonstrate their leadership and commitment to the cause and include everyone in the organization into the process by for example delegating some of the responsibility and tasks such as promotion of continual improvement to employees who don't necessarily have the top management role.

Employee awareness and training- This is a component that should be prioritized since this is a low investment with high yield. Employee awareness and training programs aim to educate employees about cyber threats, safe online practices, and the importance of cybersecurity measures. These programs should discuss topics such as: phishing awareness, password hygiene, social engineering, and data handling. By doing so, trained employees will become more attentive to suspicious activities and will have easier time recognizing some common cyberattacks. Also, this helps to mitigate one of the most common reasons for successful cyberattacks which is human error. This will also create a sense of ownership and responsibility among employees after understanding the importance of organization's digital assets.

Implementation steps

1. Establish the context

   - First and foremost, organization is to assess the current state, meaning that organization should identify needs and expectations, together with other factors that are important for achieving the desired results such as what are the current practices in regard to cybersecurity, strengths, weaknesses.
   - Identify what can help the organization towards the goals, but also what can disrupt this process.
   - Look into past data, expert opinions, and trends so that the organization can gain an understanding and strengthen their position in the process from the very start.

2. Risk Assessment

   - Identify what physical and digital assets need protection (can be digital data, software, hardware etc.).
   - Identify both internal and external factors and events that threaten the identified assets (can be human error, data leakage, weak passwords, equipment, malware, phishing, social engineering, DDoS etc.).
   - Assess vulnerabilities that can be exploited by the identified risk events.
   - Assess uncertainty by evaluating the strength of knowledge the subjective probabilities are based on.
   - Assess subjective risk probability of each identified risk event, use relevant data, expert opinions, trends, and other relevant information which can improve the knowledge.
   - Assess risk impact for each identified risk event if it was to occur, the impact can be of various types: financial, operational, reputational, legal etc.
   - Combine the subjective probability and impact in a risk matrix and evaluate the severity of risks (for example: unacceptable, tolerable, acceptable), also include the judgement of strength of knowledge and adjust severity accordingly.
   - Prioritize risks according to the severity and potential impact on the organization.
   - Implement strategies for risk mitigation to reduce probability and impact of identified risks. (Strategies to be addressed in later sections of the framework)
   - Monitor and review implemented strategies.
   - Always seek to improve on the cybersecurity front by regularly updating the assessment, be updated on recent events and trends and learn from other incidents and cyberattack attempts.

3. Educate & Train

   - Educate and train employees in the field of cybersecurity by implementing regular training sessions and workshops.
   - Educate employees on common cyber threats (phishing, social engineering, malware etc.).
   - Explain importance of following cybersecurity policies and what consequences are if one doesn’t.
   - Explain importance of strong and unique passwords.

- Train employees on how to identify phishing and other social engineering attempts.
- Require employees to report things they find suspicious.
- Explain safe internet browsing and how to identify suspicious websites, links, pop-ups, to not download unauthorized files/software etc.
- Educate employees on usage of organization's devices.
- Inform employees that simulated phishing exercises will be conducted.

4. Testing
   - Conduct exercises for phishing by creating emails that look like a phishing attempt.
   - Track when the emails are being sent out and what reaction occurs (employee reports phishing attempt, email ignored, employee fell for the phishing attempt).
5. Communication
   - Be open with the employees.
   - Provide support when a human error occurs.
   - Build trust within the organization and openly discuss cybersecurity.
   - Employees are to be comfortable to express if something is confusing to them.
6. Technological Measures
   - Implement firewalls, antivirus software, data encryption, access control system, up-to-date software, regular data backups, etc.
7. Continual improvement
   - Gather data from testing.
   - Set requirements for what results are deemed acceptable.
   - In case of unacceptable results, identify room for improvement.
   - Regularly analyze the data to monitor progress and effectiveness of the framework.
   - When significant changes or events occur assess the risks again.

Leadership

Top management is to demonstrate leadership and commitment to improve cybersecurity within the organization. Lead by example and seek to build trust and a culture that takes cybersecurity seriously. Communicate the importance of cybersecurity, be open and drive employee engagement. Emphasize the potential risks, consequences that come with it, and the responsibility everyone has in keeping the organization safe from the digital threats. Understand that gaps in expertise exist, therefore encourage open communication related to cybersecurity and pursue to create an environment where everyone feels comfortable to report incidents, share concerns and seek further explanation when needed. When top management

shows commitment, it is a first step towards building a secure and resilient organization. By highlighting cybersecurity within the organization it also builds trust with customers, partners, and other stakeholders.

Conclusion

This framework provides a simplified, but thorough approach to cybersecurity. It involves insights from risk science and from well established standard such as ISO 27001. It covers challenges SMEs face and offers simple yet effective solutions.

This framework focuses heavily on building a culture of security, promoting employee awareness and training, and conducting regular risk assessments. By adopting this framework, SMEs can become more resilient and reduce the likelihood of successful cyberattacks. The limitations SMEs often face such as lack of resources, expertise and budgets are also considered.

While this framework offers a good starting point in establishing cybersecurity in an organization, it’s simplicity also comes with limitations. The framework may not capture all the complexities that SMEs might face in their respective industries. Technology is constantly evolving and so do the cyber threats. Based on that, it is suggested that SMEs consider additional measures and adapt this framework to their needs, if possible, it is advised to seek professional guidance and consulting with experts.

5.0 Conclusion

This thesis has highlighted the cybersecurity risks of SMEs, what challenges they are facing and their current state of vulnerability. When it comes to the first part of this research question which revolves around significance of cyber threats towards SME segment, it is apparent that SMEs are very exposed and mostly do not possess required expertise or processes in place to deal with this kind of risks. It is also noticeable that SMEs do not perceive cyber threats as serious as they are, despite the impact these can cause and despite the fact that SMEs are an attractive target for cyber criminals, which is the answer to the second part of the research question of this thesis.

To answer the third part of the research question of this thesis, which is how the cybersecurity risks in SME segment should be managed, this thesis provides a framework. The framework that is presented offers a good starting point for an SME in improving their cybersecurity. It incorporates elements of risk science and is also inspired by some elements of ISO 27001. The framework has a structured approach and offers clear instructions in how to apply the process of protecting an organization from cybersecurity threats.

The future research in this field should heavily focus and dive deeper into experiences of cyberattack victims by applying a qualitative research method such as interviews which I believe would yield valuable insights into the impact of cyberattacks, as well as help identify more specific vulnerabilities and best practices to reduce these. In addition, I would suggest more focus on understanding SMEs' perception of cybersecurity risks, so that the new-found knowledge can encourage initiatives such as targeted cybersecurity awareness campaigns on a national level.

To sum it up, it is essential to understand the importance of applying risk-reducing measures for SMEs based on their specific circumstances. It creates a safer digital environment for not only the business itself, but also their customers and all other stakeholders. The end goal is to create a secure and resilient digital environment that lets SMEs operate in a "care-free" manner.

6.0 Reference List

Andreassen, I. & Brendhagen, K. (2016, October 11). Frisør presset for penger. *NRK.* https://www.nrk.no/osloogviken/betalte-losepenger-etter-dataangrep-1.13174507

Aven, T. & Thekdi, S. (2020). *Enterprise Risk Management: Advances on its Foundation and Practice*. Routledge.

Aven, T., & Thekdi, S. (2022). *Risk Science: an introduction*. Routledge.

Bailey, S. (2003). *Academic Writing: A Practical Guide for Students.* Routledge.

Bendovschi, A. (2015). Cyber-attacks-trends, patterns and security countermeasures. *Procedia Economics and Finance,* 28, 24-31. https://doi.org/10.1016/S2212-5671(15)01077-1

Carnegie Mellon University. (n.d.). What is Social Engineering?. https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html

Cloudflare. (n.d.). What is a DDoS attack?. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Cox Jr., L. A. (2008). What's wrong with Risk Matrices?. *Risk Analysis: An International Journal*, 28(2), 497-512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10), 13-21. https://www.timreview.ca/article/835

Dalland, O. (2017). *Metode og Oppgaveskriving* (6th ed.). Gyldendal.

Department for Science, Innovation & Technology. (2023). *Cyber security breaches survey 2023*. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023?fbclid=IwAR2Hk8bxtQQDy-vR5saAUTRJ1R3sAjqUVXJTKJy6xqJ7X7xGC86ru2tFv-0#contents

Fangen, K. (2010). *Deltagende observasjon* (2nd ed.). Fagbokforlaget.

Fortinet. (n.d.). What Is a Brute Force Attack?. https://www.fortinet.com/resources/cyberglossary/brute-force-attack

Gazet, A. (2010). Comparative analysis of various ransomware virii. *Journal in computer virology*, 6, 77-90. https://doi.org/10.1007/s11416-008-0092-2

Guevara, P. (2023, June 6). A Guide to Understanding 5x5 Risk Matrix. Safety Culture. https://safetyculture.com/topics/risk-assessment/5x5-risk-matrix/

Hove, S. E., Mollan, A., & Ehsas, P. (2022, November 13). Hvem bærer risikoen for cyberangrep?. *Finansavisen.* https://www.finansavisen.no/nyheter/debattinnlegg/2022/11/13/7958510/debatt-hvem-baerer-risikoen-for-cyberangrep

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, 15(4), 2091-2121. 10.1109/SURV.2013.032213.00009

Lewis, J. A. (2006). *Cybersecurity and critical infrastructure protection*. Center for Strategic and international Studies. Retrieved from https://www.csis.org/analysis/cybersecurity-and-critical-infrastructure-protection

Madani, A. E. (2018). SME policy: Comparative analysis of SME definitions. *International Journal of Academic Research in Business and Social Sciences, 8(8), 103-14. https://doi.org/10.6007/IJARBSS/v8-i8/4443*

Mathisen, G. (2022, September 23). Hackerne holdt på å knekke Emberland. *Maleren.* https://www.maleren.no/cyberforsikring-hacking/hackerne-holdt-pa-a-knekke-emberland/298132

Nærings og handelsdepartementet. (2012). Små bedrifter-store verdier: *Regjeringens strategi for små og mellomstore bedrifter*. Retrieved from https://www.regjeringen.no/globalassets/upload/nhd/vedlegg/rapporter_2012/102377_nhd_smb_web.pdf

Næringslivets Hovedorganisasjon. (n.d.). *Fakta om små og mellomstore bedrifter (SMB).* https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/

Næringslivets sikkerhetsråd. (2022, September 20). *Mørketallsundersøkelsen 2022.* Retrieved from https://www.nsr-org.no/aktuelt/morketallsundersokelsen-2022-er-na-tilgjengelig

Nasjonalt cybersikkerhetssenter, (n.d.). Digital Sikkerhet. https://nsm.no/fagomrader/digital-sikkerhet/

Nasjonalt cybersikkerhetssenter, (n.d.). Nasjonalt Cybersikkerhetssenter (NCSC). https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

Nasjonalt cybersikkerhetssenter, (n.d.). Norwegian National Cyber Security Center (NCSC) and NorCERT. https://nsm.no/areas-of-expertise/cyber-security/norwegian-national-cyber-security-centre-ncsc/

Nasjonalt cybersikkerhetssenter, (n.d.). Vi opplever nå et dataangrep, hvem kan hjelpe oss?. https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/digital-utpressing/vi-opplever-na-et-dataangrep-hvem-kan-hjelpe-oss

Palo Alto Networks. (n.d.). What is Malware & How to Stay Protected from Malware Attacks. Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-malware

Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know?. *International Business Review*, 29(4), 101717. https://doi.org/10.1016/j.ibusrev.2020.101717

Pettersen, R. C. (2008). *Oppgaveskrivingens ABC: veileder og førstehjelp for høgskolestudenter.* Universitetsforlaget.

Politiet, (n.d.). Datakriminalitet. https://www.politiet.no/rad/datakriminalitet/

PwC. (2022). *Cybercrime survey 2022*. Retrieved from https://pwc-norway.viewer.foleon.com/publikasjoner/cybercrime-survey-2022/

Rahmonbek, K. (2023, February 22). 35 Alarming Small Business Cybersecurity Statistics for 2023. *StrongDM.* https://www.strongdm.com/blog/small-business-cyber-security-statistics#small-business-cybersecurity-overview

Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World*. New York: Earthscan.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students* (8th ed.). Pearson.

Standard Norge. (2023). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements* (NS-ISO/IEC 27001:2022). https://handle.standard.no/nettbutikk/sokeresultater/?search=NS-ISO/IEC+27001+2022

Thagaard, T. (2018). *Systematikk og innlevelse: en innføring i kvalitative metoder* (5th ed.). Fagbokforlaget.

Tufte, P. A. (2014). Kvantitative metoder. In K. Fangen & A. Sellerberg (Red.), *Mange ulike metoder*. (p. 71-99). Gyldendal.

Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. *International Journal of Network Security*, 15(5), 390-396.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38, 97-102.* https://doi.org/10.1016/j.cose.2013.04.004