FACULTY OF SCIENCE AND TECHNOLOGY

MASTER THESIS

Study programme / specialisation:

The spring semester, 2022

Open

Author:

Vetle Tengesdal Torstenbø & Johnny Øvrehus

(Signature author)

Course coordinator: Eirik B. Abrahamsen

Supervisor(s): Ole Andreas Engen

Thesis title: Cyber-threats against the Norwegian financial sector

Credits (ECTS): 30

Keywords:

Cyber-threat, cyber-attack, complexity, ISO27001, NIST, robustness, resilience, redundancy, financial sector, value chains, vulnerability, risk, digitalization, development, personal information, GDPR, cyber-crime, human factors

Pages: 66

+ appendix: 80

Stavanger, 13.06.2022
date/year

Cyber-threats against the Norwegian financial sector

Master thesis Risk Analysis

University of Stavanger

June 2022

Vetle Tengesdal Torstenbø

Johnny Øvrehus

Preface

Neither of us could have predicted that our two vastly different academic backgrounds would bring us together as it has. This assignment has given us knowledge that we can take with us. By carrying out such a task, we have had the opportunity to dive deeply into a current and exciting topic, namely cyber threats. Together with the rest of the master's program in Risk Analysis, we feel well prepared for future challenges.

We would like to thank our supervisor, Ole Andreas Engen, who got us started early with the work required with such a thesis and has always had faith in us as students. With the help of his chronic and contagious optimism, he has really been of tremendous help.

Many thanks to family, friends, girlfriend, and wife for enduring and always having faith in us through a demanding course of study with both pandemic and home school.

Vetle Tengesdal Torstenbø

Stavanger,
June 13, 2022

Johnny Øvrehus

Stavanger,
June 13, 2022

ABSTRACT

Technological development affects most of the industries in the world, and the Norwegian financial sector is no exception. We use our digital tools every day, and these tools make footsteps of personal information. Norway is one of the most digitalized countries, and digitalization has brought new ways of thinking and made the sector more effective. However, this also brings new challenges with new vulnerabilities and risks. All this has made a need for understanding and managing cyber-risk.

This thesis investigates how the Norwegian financial sector handles the risk of losing personal information when drawing on cyber-attacks by performing a content analysis based on relevant documents and articles. Discussion and analysis of the dominant documents and articles contribute to achieving the thesis goal of answering the research question. We do this intending to generate awareness of the cyber-risk in the sector when it comes to handling personal information. Additionally, we aim to create an understanding and knowledge base of the topic to understand the development better and be capable of being resilient to this type of risk.

The content analysis of cyber-risk and cyber-threat in this thesis reveals that the risk of losing personal information is in constant flux. The reason is compound, but the analysis shows that our main findings can summarize it; Implementation and enactment of complexity in existing material, Speedy development and an arduous environment, and Endorsement of robustness, relicense, and redundancy.

We were especially boggled over the neglection of integrating complexity as a risk in both the current NIST-framework and the ISO27001 standard. Also, the rapid development of technology and different types of actors may force the sector to take measures, but the long value chains increase the complexity.

Table of content

Figures:

Tables:

1. Introduction

1.1 Background

In the autumn of 2020, several cyber-attacks were carried out against the Norwegian Storting and other Norwegian organizations. The Norwegian Police Security Service (PST) investigation revealed that the espionage group "Fancy Bear," also known as APT-28, was to blame for the cyber espionage. This group is part of the Russian military intelligence service – Glavnoje Razvedyvatelnoje Upravlenije (GRU). The group has also apparently been involved in many targeted operations, like cyber-attacks on international sports organizations, government agencies, and national assemblies in many other countries. By attacking the Norwegian Storting, the Russian group succeeded in stealing sensitive information from several email accounts. Sensitive information like this, which has come into the wrong hands, can be used to influence individuals or political processes (PST, 2021).

In Norway, all companies are obliged to comply with the Personal Data Act and stipulate that all companies should have a complete overview of their processing of personal data and implement technical and organizational measures that ensure that the law complies. Each company should make essential assessments on its own before collecting and using personal information. The company is also responsible for documenting that they comply with the law. Violation of the rules can lead to sanctions, such as warnings, reprimands, bans, and orders. Today, cyber-attacks are no longer stopped by antivirus software or firewalls. The risk of cyber-attacks is constantly increasing, and for companies and institutions, it is no longer a question of "if" it will happen but rather "when." Therefore, cyber security is essential (Visma, n.d.).

The knowledge of risk

Based on Terje Aven and Ortwin Renn (Aven, 2020), the SRA (2018) defines risk as "the effect of uncertainties on objectives." In contrast to many other definitions of risk, uncertainty has replaced probability. The idea is that we face risk when we operate a process plant or make an investment, independently of whether this risk has been measured or not. The main point of Aven and Renn (Engen et al., 2016) is that the concept of risk must be based on uncertainty beyond a quantified probability. We should not define the concept of risk using one specific measurement tool, i.e., probability. Numerating probabilities can be a practical tool, but

uncertainty will always be associated with the probabilities one calculates. Risk analyses based on probability calculations are not useless. However, the utility value depends on whether the risk analyses are based on excellent and realistic assumptions and valuable information and knowledge. Another essential principle highlighted by Engen et al. (2016) is risk management. By distinguishing between complexity, uncertainty, and ambiguity in risk, it is possible to develop different strategies for risk management. The relevant information and the assessments gathered in the previous phases are used here.

Aven (2017) divides risk management into two diverse types. The A type of knowledge is knowledge related to an activity (interpreted in a broad sense also covering natural phenomena) in the real world, for example, the use of a medical drug, the design of an offshore installation, or the climate, whereas the B type knowledge on concepts, theories, frameworks, approaches, principles, methods, and models to understand, assess, characterize, communicate, and (in a broad sense) manage risk. A part of knowledge is generated through multidisciplinary and interdisciplinary activities. Risk analysis supports other disciplines—the natural sciences, engineering, medicine, etc.—with risk-related concepts, methods, models, etc. For B type of knowledge, this part is genuine risk analysis because no other fields or sciences address this task on a generic level. The B part is, on the other hand, rooted in generic questions and problems concerning, e.g., how to conceptualize and measure risk, how to understand why lay persons' risk perception could differ strongly from professional risk analysis judgments, how to best communicate risk, how to make sense of the precautionary principle, how to best compare benefits and risk, how to make use of cost–benefit analysis in risk analysis, etc. Aven writes that risk management covers all measures and activities carried out to manage and govern risk, balancing developments and exploring opportunities, on the one hand, and avoiding losses, accidents, and disasters, on the other. They are essential when choosing between the A or B type of knowledge. The risk analysis field generates knowledge based on A and B. The risk analysis science generates scientific knowledge according to A and B, where scientific refers to the most warranted (justified) beliefs or statements that the risk field produces. This thesis will spotlight the B type of knowledge, focusing on generic questions and problems and how to conceptualize and understand risk.

The digital revolution

The world has evolved in a digital direction for a long time. This direction has led to independence and freedom that brings benefits and relief. During the ongoing global pandemic, the digitization of work tasks has been necessary to avoid infection while providing employer and employee security. *Digitalization* is defined as the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business (Gartner, n.d.). Even though digitalization gives us a range of opportunities, it also presents us with challenges. New challenges provide us with new risks, threats, and vulnerabilities. This involves us all and could significantly impact our privacy, e.g., all the technology we are surrounded by. Once the offender has the motivation and knowledge, we become more vulnerable as users of digital tools (Elmaghraby & Losavio, 2014). Although digitalization gives freedom, there are at the same time several things that give great uncertainty about using digital tools. However, safety connected to technology is not a new thing.

Cyber-security´s priority and evolvement

Since 1990, the Norwegian National Security Authority (NNSA) has helped organizations with security-graded information systems. But there has been a massive development concerning technology since the 1990s, and our society has gone from an analog society to a digital one (NNSA, 2022). Still, technology is constantly evolving and will be for a long time, and therefore complex to determine when this change will stagnate. Confederation of Norwegian Enterprise (NHO) claims that digitalization will change society, business, and working life in several crucial ways in the year to come (NHO, n.d). As the digital vulnerability in society grows, it will lead to increased concerns for society, as PST refers to in their reports dealing with the risk picture for Norway (PST, 2021). The risk picture faces a change of pace in digital risk in Norway. The number of serious incidents registered with the National Cyber Security Center (NCSC) in the Norwegian National Security Authority (NSM) in 2020 was three times as many as in 2019. NCSC has observed a significant increase in incidents related to encryption viruses and financially motivated online crime in the past year. At the same time, advanced players still carry out complex espionage operations against Norwegian targets, including where our most important values are managed. This has consequences for Norway's state and social security (NSM, 2021). Our issue will be based on the growing trend in cyber security and how it threatens privacy (GDPR) in the Norwegian financial sector. We want to map trends and patterns associated with this development in the financial sector. To do this, we will have a

historical approach to risk where threats and dangers to privacy in financial sectors are the object of study.

Considering cyber-risk, several actors are experiencing a higher level of vulnerability. Although, the risk picture is in constant change. Due to this, we find the Norwegian finance sector's laws and regulations regarding the Private Data Act interesting concerning complexity. This sector involves public and private actors and has a curtail function in Norwegian society. Additionally, if personal information goes astray, this can cause significant consequences, both financial and reputational. The Norwegian financial sector also handles central economic values, which makes the sector tempting and worthwhile to attack for hackers.

Is complexity our new enemy?

Systems tasked with managing and ensuring privacy are complex. They have an essential task that is not always easy to handle. The fact that the systems are complex means that several factors come into play, which can lead to weaknesses or breaches of private storage. Perrow (Engen et al., 2016) states that complex systems have proximity between parts and units that do not belong together, creating unforeseen interactions. In addition, such systems are characterized by many interactions between parts, units, and subsystems that are not part of the production process or planned. This creates large numbers of control parameters, complex information flows, and challenges related to operators' understanding of processes. It is possible to imagine control solutions for tightly connected and complex systems. If the risk analyzes are rational and scientific enough, at the same time as the organizations that manage the technology have clear routines, and close follow-up, the "errors" that can lead to disaster will be eliminated. Perrow problematized this and claimed that intricately connected and complex systems represent a management dilemma. Complex and loosely connected systems are best managed through decentralized management. There are thus no obvious organizational solutions for how tightly connected and complex systems are to be managed (Engen et al., 2016).

First, the companies' systems may be too weak and unstable to handle a hacker attack. Data hacking is one of the most significant information security risks organizations face, and sensitive data is used across all business areas, increasing value. Countless incidents occur every month, whether cyber-criminals hack into a database or employees who lose or misuse information. No matter where the data goes, the financial and reputational damage caused by a

breach can be devastating. In addition, the method deals with the customer, where for example, a hacker sends an email that gives the hacker access to personal information (Engen et al., 2016).

Interconnection and increased interaction within systems could make organizations more vulnerable to accidents associated with cyber-attacks and the risk management process concerning these events (Engen et al., 2016). Based on Rosa, Renn, and McCright (2014), risk management in today's risk society is seen as the scope and complexity, and the global nature of risk plays out the existing and conventional methods that deal with them.

Recent security research suggests most companies have unprotected data and poor cyber-security practices, making them vulnerable to data loss. To successfully fight against malicious intent, companies should make cybersecurity awareness, prevention, and security best practices a part of their culture (Sobers, 2021). Three key terms are used in connection with information security:

- Confidentiality (that the information is not made known to unauthorized persons)
- Integrity (that unauthorized persons do not change the information)
- Accessibility (that the information is authorized when necessary)

See chapter 5.3.2 for more details.

1.2 Topic question

In this thesis, we aim to investigate how the Norwegian Financial Sector has developed regarding cyber risks, threats, and dangers. We do this with a historical approach and focus on General Data Protection Regulation (GDPR), laws, regulations, and relevant framework and standard. The purpose of the paper is to elaborate on how the sector handles the risk of losing personal info and then establish patterns concerning the development and digitalization in the sector. The topic question that covers the assignment is the following:

Drawing on cyber-attacks, how is the risk of losing personal information handled by Norwegian financial sector?

By elaborating on this question, some sub-questions have been developed that highlight and justify the topic question. The first sub-question investigates the continuous change in risk management and cyber-attacks. This is essential to cope with the change in threats and dangers

for the Norwegian finance sector. Will threat change possibly evolve into other risks and risk descriptions? This leads us to the first sub-question:

How does continuous change of cyber-attack influence risk descriptions in the financial sector?

Furthermore, threats may not exclusively be risks seen by the naked eye but also connected to systems and their complexity. This will be essential to examine and determine how the sector acknowledges this, especially concerning the current framework and the ISO27001 standard. This leads us to the second sub-question:

How does risk management handle increased systemic complexity?

To fully understand how the Norwegian Financial Sector handles the risk, it is vital to recognize and explain why the cyber-threat implies the risks against the sector. Based on this, the last sub-questions are formulated as follows:

Why do cyber-threats impact risk, risk analysis and risk management in the financial sector?

1.3 Limitations

By answering these questions, we aim to discover challenges with the current framework and standard regarding cyber-security and GDPR, focusing on complexity. In the current framework, we find it strange that it is a lack of focus on this topic. Therefore, this thesis will hopefully contribute to further developing the current framework and standard. The limitation in the thesis we envision is that we focus on an overall image, not a specific business or enterprise. We envisage further narrowing the task to focus on how companies protect their employees and customers against breaches of privacy regulations. In this assignment, we have limited the period to 5 years. This provides an insight into how the sector has developed and continues to change. By making these limitations, we aim to thoroughly analyze a topic that has not been studied enough before and lacks scientific work. However, the main focus of this thesis will be on the Norwegian financial sector. We see that scientific work can be relevant for other sectors as well.

1.4 Relevance

This thesis will give an answer to a relevant problem for today's society and the Norwegian financial sector. The new privacy law has obliged all organizations and businesses to familiarize themselves with the new requirements, a continuation of the previous law that dealt with the same principles. Problems with GDPR and privacy security involve risks, handling of personal information, risk consequences, etc. Therefore, high political requirements are required to help give the Norwegian financial sector tasks that will make their systems resilient and robust. If the various companies manage to create and operate both resilient and robust systems regarding GDPR, they have come a long way. It is a good start, but several factors come into play.

Cyber-security constantly changes and is a constant threat to the Norwegian financial sector. As mentioned at the beginning of the introduction, the Norwegian Storting experienced several cyber-attacks in 2020. The implications of these attacks were the loss of sensitive information. Since this was an attack carried out by GRU, it displays that sensitive information is valuable and can be misused when it falls into the wrong hands. This shows us that a resilient and robust system is needed for organizations to withstand such attacks and shows its relevance in a digital world. In addition, new regulations and legislative changes make the work with cyber-security more advanced, but at the same time provide both organizations and customers with more security if these are followed. The connection between the imposed changes and the constant change in the threat picture can be factors that play a role in increasing the complexity of security. Annual threat assessments are made by both PST and NSM, which deal with national security. However, few or none address the perspective of complexity and privacy information in the financial sector in an ample way.

Moreover, the use and necessity of storing personal information increases. Are the current frameworks good enough to handle this? This makes the task truly relevant for both organizations and society in general. The professional relevance will be elucidated using theory from the risk field of science regarding risk elements.

1.5 Previous research

Cyber-security is a relatively new field that is constantly evolving. That makes it a field that has not been studied to the desired extent, at least when it comes to research that deals with the financial sector and handling personal information when the complexity is involved. Previous research in this field helps to indicate how the financial sector in other countries handled the transition from an analog system to the revolutionary digital universe. This chapter will briefly present the three most relevant articles previously published, and these articles will be applied in chapter 6.

International Monetary Fund (IMF)
"Cyber Risk for the Finance Sector: A Framework for Quantitative Assessment."
Bouveret 2018

In his research, Antoine Bouveret (2018) claims that cyber risk has emerged as a critical threat to financial stability. By analyzing diverse types of incidents like data breaches, fraud, and business disruption, the paper presents documentation of cyber risks worldwide for financial institutions. Bouveret suggests using a quantitative framework to assess cyber risk for the financial sector, which assesses several types of stability risk. By this, the framework can be applied at the individual country level. The findings presented show the cyber risk to be growing and intensifying.

Furthermore, cyber risk is considered one of the critical factors regarding financial stability for financial institutions. Hence, the following recent attacks on financial institutions. Additionally, the paper addresses private as well as public actors.

This article contributes to our thesis by focusing on how cyber a key threat to financial stability, which is a focus point in this thesis. Furthermore, inspiration was found in the way Bouveret addressed a quantitative framework to highlight cyber risk. This made us aware of the importance of a solid framework that describes and calculates cyber risk.

“The General Data Protection Regulation in Financial Services Industries: How Do Companies Approach the Implementation of the GDPR and What Can We Learn From Their Approaches”?
Holler et. al. 2020

This article aims to explore the GDPR in financial services. By investigating a three-stage iterative and risk-based implementation approach, good practices for implementation at various levels were unveiled. Nevertheless, the case study, which involves leading financial companies, uncovers that the companies strive with the most effort to ensure compliance with the GDPR. However, the paper claims a gap exists between strategy and implementation. This gap becomes evident as an enterprise conducts assessments, creates strategies, and develops frameworks. However, they neglect the existing information technology.

Holler's paper is relevant for this thesis because it improves individuals' ability to control information recorded about themselves. GDPR is necessary since it is a statutory point as the Norwegian financial sector should take into account to store and handle personal data.

“A multi-level approach to understanding the impact of cybercrime on the financial sector”
Lagazio et. al. 2014

To understand the impact of cyber-crime in the financial sector, the paper suggests a multi-level model based on system dynamics methodology. This being coherent with recent findings, the paper's results show that solid dynamic relationships affect cyber-crime cost and occur at various levels of society and value networks. Unwanted consequences such as weak policing, weak international frameworks, and increased jurisdictional arbitrage opportunities for cyber-criminals can increase the cost.

What we find interesting in this paper is that Lagazio, like IMF, highlights the importance of a robust framework. Lagazio writes about weak international frameworks, and we have taken inspiration from this way of thinking since the financial sector currently handles cyber-risk with frameworks and standards.

1.6 Structure

In this thesis, several vital themes in research will be reviewed. Chapter 1 will introduce the theme, problem issues, research questions, and how we aim to delimit the paper. Chapter 2 gives us the context of the paper. This is also where the framework is set for the task. In this chapter, the cyber security and digitalization of the finance sector in Norway will be accounted for, with its demands and regulations. For this paper, the GDPR regulations will be highly relevant. Chapter 3 is the clarification of the used theories and concepts that are used in the discussion in the paper. In chapter 4, the method is elaborated upon. A review of our choices will be included throughout the process.

Furthermore, clarification and elaboration on the quality of the materials used are provided. Chapter 5 presents our findings and empirical work. This will be relevant in chapter 6 with our discussion. To summarize, chapter 7 will provide the main findings and answer questions provided in the paper. In the end, suggestions for further research will be provided.

2. Context

The digitalization of the Norwegian finance sector has affected customers and employees in everyday life, and the sector has undergone dramatic changes in recent years. Technology, evolution, and development are constantly changing, providing new challenges every day. Based on statistics from NCSC, severe events in 2020 were three times higher than in 2019. NCSC observed a significant increase in events concerning different viruses and economically motivated crime over the years (NSM, 2021). In this chapter, the sector's digitalization will be presented alongside cyber-security. Laws and regulations will also be explained regarding cybersecurity and digital development.

2.1 Cyber-security in the financial sector

Cyber-security is a relevant and necessary topic to explain since technological development has changed the risk picture and created new vulnerabilities that need to be dealt with. Cyber-attacks come in many forms and threaten financial stability in the worst-case scenario since the financial systems cannot cope with the disturbances, recover errors, and ensure that critical economic functions in society work (Hægeland & Kongsrud, 2019). The main point of a cyber-

attack is to hurt, disturb or outrun the systems, so the users do not gain access so that the hacker can get money or sensitive information. Bowcut (2021) states that by gaining access to personal information, a hacker can get the customer's home address, social security number, banking details, phone number, email address, and income information. The high value of this data on the darknet makes this sector an attractive target for cyber-criminals.

An essential aspect of the foundation of financial services is trust. Organizations aim to win and maintain the trust of their customers. To do so, financial institutions should demonstrate dedication to preserving confidentiality, confirm the availability of systems and services, and maintain data integrity. However, maintaining trust has never been more challenging than it is today. There has been a change in cyber-security threats, where they have moved from attacks on individual institutions to attacks on the financial system. The financial sector is transforming with new digital channels, automation, and other advanced technologies, introducing real benefits and new risks. To protect the systems, regulators are focused on systematic cyber-risk and contagion across firms and third parties. They also expect financial institutions to enhance privacy protection for customers who demand their confidential information to be well protected across digitally accessible products and services. With this integration, the financial institutions will achieve positive business outcomes, effective risk management, and deliver and maintain trust in the financial market (Doe, n.d).

2.2 Digitalization in the financial sector

The Norwegian financial sector has undergone dramatic changes in the last 20 years. The sector has been gradually released from the Norwegian state, financial institutions have been permitted to establish business abroad, and foreign actors have been given access to the Norwegian finance market (UIO, 2003).

Norway is a digitalized society. Norway is one of the most digitalized countries in the world, and according to the Digital Economy and Society Index (DESI-index), Norway is ranked number five in the world by the European Union (European Commission, 2021). The DESI-index measures digital competence, the use of digital services in business and society, and public digital services. With this index in mind, we can say that Norwegians are suitable to address and use modern technology and that solutions have been made by using the technology in the development of society.

One of the biggest revolutions in the history of digitalization in the financial sector was the entrance of the internet at the beginning of the 1970s (Aion digital, 2020). This revolutionized how information and communication could be handled, especially in the financial sector. Usage of the internet is a massive part of today's society. This forces the sector to change the way the sector operates and calls for a much more developed digital way of thinking. This has forced the sector to be innovative when facing recent technologies and digitalization. One example of this is the innovation of the "cash-less" society, with the example of Apple Pay (Apple, 2021). This means we are moving away from using cash to just using our technology when we will pay for something.

Innovative technologies and expanding attack surfaces enable a more dangerous and diverse cyber-crime range (WEF, 2022). According to the World Economic Forum (WEF), this puts even more strain on financial institutions, and its rapid digitization risks expose economies to new and more intense cyber vulnerabilities. Additionally, with the recent Russian cyber-attack on the Norwegian Storting, which succeeded in stealing information, it is demonstrated that the challenges in digitalization can provide consequences to the sector. Even though digitalization and technology generate immense benefits, we should to the highest extent, try to make sure that we understand the implications of digitalization in the financial sector.

2.3 General Data Protection Regulation

A new law on personal processing data was passed on the 15th of June 2018 and entered into force on the 20th of July 2018. The new law implements the EU Privacy Regulation (GDPR) in Norway and makes the Norwegian regulation law (Kommunal- og distriktsdepartementet, 2019). The primary purpose of the regulation and the Personal Data Act is to safeguard the individual's privacy when facing electronic interaction of personal information. The Personal Data Act will be further described in chapter 3.3. Also, an essential aspect of the regulation is to achieve equality in treating personal information in the EU, not only in Norway. The significance of GDPR will impact how institutions like the financial sector secure and treat personal information (UNIT, 2020). With this security of information, it is the ability to prevent, detect and deal with events that can lead to violation of confidentiality, integrity, or availability.

In this thesis, we aim to help us better understand the value of personal information and how the financial sector copes with the constant threat of preventing the information from falling into the wrong hands. Although this paper is not about legal objects, we need to look at both aspects of GDPR and informational safety to fully comprehend and understand the situation concerning risk.

2.4 Laws and regulations

Organizations like the financial sector must follow several laws and regulations to deal with digital security. Norway came on the scene early in digital security, and the first report came as early as 2003. It has been revised several times over the years, and in 2017 Norway received its first Official Norwegian Reports (NOU) exclusively on digital security (Kommunal- og distriktsdepartementet, 2019). In NOU 2018: 14, the Ministry of Justice and Emergency Preparedness comes with recommendations for socially critical businesses. NOU 2018:14 gives requirements for notification of undesirable digital incidents, and guidance must be provided to the law, at the same time as requirements are set for helpful information and communication technology (ICT) security. They want the NOU 2018:14 to implement the Network and Information Security (NIS) -directive in Norwegian law (Justis- og beredskapsdepartementet, 2018).

The NIS-Directive was adopted in the EU in 2016 and required the Member States and the EEA countries to ensure that a certain level of ICT security is maintained. This is done by creating a strategy for security work, establishing an ICT security contingency unit (CSIRT), and imposing ICT security requirements and notification obligations on operators and suppliers of socially necessary services. The notification only applies in the event of severe ICT breaches. The directive was created because the EU does not implement sufficient, comprehensive protection measures to ensure and maintain reasonable enough security in networks and information systems within critical infrastructure. The NIS Directive has mentioned seven services essential for maintaining a functioning internal market. If they lapse, it can seriously negatively affect social security, economic, and social activities. Here, the financial market infrastructure is one of the points and shows the importance of a robust and resilient sector (EØS-notatbasen, 2016).

3. Theory

In this chapter, we will review relevant theories to find connections between our problem and our sub-questions before looking them up against each other in the discussion chapter. In the first part of the chapter, we will account for clarifications of concepts. Second, we will present the National Institute of Standards and Technology's (NIST) cyber-security framework. Further on, we will review the privacy risk management framework by Andrea Tang. Next, Charles Perrow's National Accident Theory, Erik Hollnagel's theory regarding complexity and resilience, and the Privacy Information Act will be presented. These theories are relevant for this thesis and should be included to understand and justify the topic question's relevance fully. We acknowledge these theories due to the importance of current paradigms that are used by industry. This thesis will analyze and discuss how the Norwegian financial sector handles privacy breaches. At the same time, it will look at whether the frameworks from NIST are good enough or whether they should implement or exclude some parts. In the frameworks that are used today, complexity is not an essential part and is mentioned once in NIST's framework. This is a critical factor that comes into play when handling cyber security for the Norwegian financial sector due to the complexity of the systems they use. Perrow's theories and views will, in this thesis, be used as an argument to include complexity as a new crucial point in the current framework. It will help to increase the Norwegian financial sector's understanding of handling cyber-attacks while at the same time increasing the quality of the framework. The theories presented in this chapter will then be reviewed and used to answer our questions.

3.1 Clarification of concepts

3.1.1 Risk

Several risks come into play when it comes to managing privacy. In line with SRA (2018), it is impossible to define risk in one sentence. They have agreed upon seven definitions of objectives that are essential regarding the definition of risk. On the other hand, ISO31000 defines *risk* as “the effect of uncertainties on objectives.” (ISO, 2018). However, we acknowledge that risk is also defined in the ISO31000 standard. However, as Aven (2020) claims, it is poorly formulated because the risk concept is so tied up with formulations of objectives. Managing risk in privacy is challenging, especially when it comes to handling. Many industries see this as demanding, and as Kruse et al. (2017) claim, this also includes the healthcare industry with its difficulties identifying new and the constant change in threat scenarios.

The risk may arise when we use technology to store, send and process information when dealing with information security. In a specific information security environment, we may define *risk* as: "The potential for a given threat to exploit vulnerabilities to gain unfair access to a value or group of values and thus cause harm to the organization." However, in this thesis, we will refer primarily to the value of information. Due to the vast amount of information and economic assets the financial factor handles daily, we acknowledge the importance of assessments to be aware of the danger to this value (NTNU, n.d.).

We chose to specify this topic because we find the definition lacking information and formulation regarding the topic of "cyber-risk." We find it essential to acknowledge this for us to investigate further and enhance the definition of risk, allowing us to dig deeper into finding appropriate ways to handle the risk. This enabled us to detect and envision the importance of the three-factor model as a tool for risk analysis.

3.1.2 Three-factor model

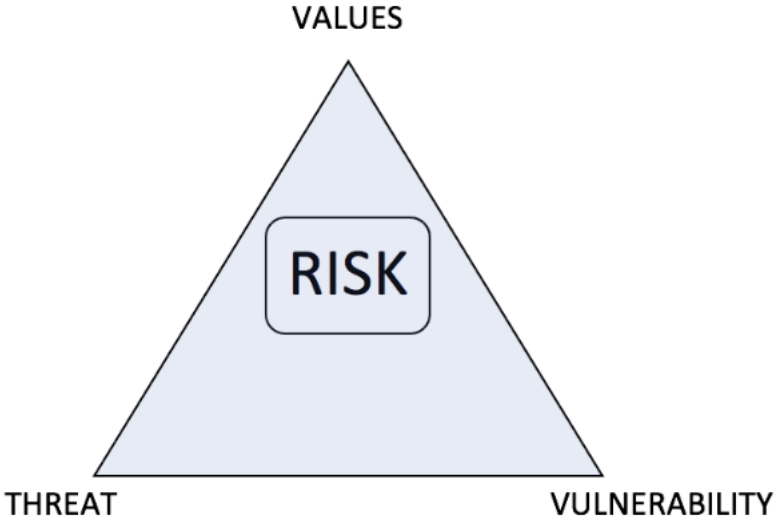

Figure 1

Three-factor model (TFM)
(Busmundrud, Maal, Kiran & Endregard, 2015)

The figure shows us the impact of different factors that are all important to risk. The intervention of the factors will play a role in handling risk. Based on these three parameters, we can find a risk level. However, this model does not consider the probability of a scenario occurring. To give an example of a risk assessment, the table below shows the different factors that make the parameters. This shows us the different values, vulnerabilities, and threats involved in the assessment. Additionally, this can be translated into different scenarios, like the financial sector and other sectors, for example, the health sector.

Values	Vulnerability	Threat
- Life and health - Operational capability - Sensitive information - Reputation	- Technological (security, "barriers") - Organizational (instructions, process descriptions, organization, unwanted actions are detected) - Human (education, attitudes, prevention)	- Penetration - Interception - Theft of information - Explosions - Armed attacks - Infrastructure destruction

Table 1

Examples on values, vulnerability, and threat
(Busmundrud, Maal, Kiran & Endregard, 2015)

Threat

Based on Aven (2020), a *threat* is defined as "*a stated or inferred intention to initiate an attack with the intention to inflict harm, fear, pain or misery*," while Oladimeji et al. (2006) define a threat as "*simply a potential violation of the security of a system - an event that may have some negative impact*."

In the financial sector, the threats are widespread, with several types of actors with different interests and intentions carrying out an attack. In this thesis, the threats that will be our focus will concern actors intentionally carrying out attacks to congregate information unlawfully.

Also, the unintended consequences of threats will be understood as a "threat," for example, when we elaborate on Perrow´s work on complexity. Based on NIST, we will define a "threat actor" as one actor with the capability to cause unwanted harm (Stine et al., 2020). In cybersecurity, as in the example in table 1, there are many different actors, but our focus will be on cyber-criminals that carry out attacks meant to steal data and personal information. We acknowledge this as a critical factor due to the diversity of different actors and criminals with different intentions.

Vulnerability

In line with risk, vulnerability also comes with various aspects of approaches when used. In our case, vulnerability is actual security weaknesses or flaws that make a system susceptible to an attack. An attack exploits a vulnerability to realize a threat (Oladimeji et al., 2006). On the other hand, vulnerability is the opposite of robustness. Like Aven et al. (2004) claims, robustness is "a system's ability to withstand and maintain its function in various forms of external influences." In this thesis, we aim to elaborate on how the financial sector copes with this vulnerability and connect this to cyber security.

More complex systems with addiction to digital and electronic information systems and tightly linked systems make us vulnerable due to the constant and new environments (NOU 2000:24). Additionally, connect this vulnerability through compromised confidentiality and integrity. This also includes safety measures, both technical and organizational, to secure the system and information. Furthermore, it is about implementing risk-reducing measures and barriers to avoid unnecessary events developing and producing significant consequences. Besides, we also acknowledge the link between robustness and resilience. While robustness is the system's ability to withstand and maintain, resilience, despite the lack of consensus on an operational definition, can be defined as the ability and capacity to regain from difficulties (Herrman et al., 2011). With this in mind, we acknowledge the importance of these differences in vulnerability. Due to the complexity of the surroundings involved, we see this as a critical part of the theory in this thesis.

Values

In the Norwegian Financial sector, we uncover many different values. They can be decided on their meaning regarding decisions, assessments, and measures taken to secure and protect them. A primary value could be information and work processes, and secondary values can be

hardware, software, network, and personnel (Røv, 2021). Engen et al. (2016) show the TFM that could be used in risk analysis when handling threats. The model includes a value-a threat- and a vulnerability consideration. These factors unite a risk connection between consequences and probability and present the risk picture. They are crucial when deciding which measures to implement to reduce a threat. It is a Norwegian model based on supervisors from the NSM, the police directorate, PST, and Norwegian Standard 5832. A good feature of the three-factor model is that it can be used in safety and security principles and may soundly suit our topic question. It suits this thesis because of the constant change in threats and dangers and the balance between the two dimensions. Aven believes a risk assessment is based on value, threat, and vulnerability dimensions. His main point is that one should use safety and security concepts that adequately address uncertainty dimensions. Uncertainty is described through capacity, intention, probability, and knowledge strength. The differences between the safety and security dimensions show the importance of universal acceptance of good and precise concepts, which will be explained in the next chapter.

3.1.3 Safety and security

There is a gap between security and safety that needs to be clarified. Aven (2020) defines safe as being without unacceptable risk, and safety is interpreted similarly. It is possible to talk about safety as the antonym of risk; therefore, an elementary level of safety means a low level of risk. *Security* is defined as being without unacceptable risk when restricting the concept of risk to intentional unwanted acts by actors. Security can be interpreted in the same way as to secure and as the antonym of risk when restricting the concept of risk to intentional unwanted acts by actors. The security level is also linked to the risk level, and a high-security level means a negligible risk. Boholm et al. (2016) claim that the TFM can be seen considering both safety and security perspectives when the threat has the potential to harm essential values. We also see this as an important part of our thesis. Information is a significant value and should be seen considering safety and security.

The risk management process has a solid connection to safety and security and needs to be considered when managing risk. Additionally, using a safety perspective, the threat can be understood as an unintended event (like dangers) and, from a security perspective, will be understood as an intended event. Besides, the security term will also be elaborated on when it

comes to both resilience and robustness and when we give voice to actions that are intended to do harm.

3.1.4 Risk management

The practice of risk management became widespread in the 1950s because of cost insurance since it was both prohibitive and the extent of coverage limited. Many organizations realized that purchasing insurance in the 1950s was insufficient if there was inadequate attention to protecting property and people. They, therefore, became concerned with the quality of property protection, the standards of health and safety, and other risk control concerns. When the risk management approach became established, it also became clear that organizations faced many uninsurable risks. The approach is now such that the links with insurance are much less robust. Insurance is seen as a risk control technique and is only applicable to a portion of hazard risks. It is difficult to provide a universally accepted definition of risk management since it is difficult to agree upon a universal definition of risk. Hopkin defines *risk management* as "*Risk management is the set of activities within an organization undertaken to deliver the most favorable outcome and reduce the volatility or variability of that outcome.*" In contrast, the Institute of Risk Management (IRM) defines it as a "*Process which aims to help organizations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure*." We can see there is a disagreement between scholars (Hopkin, 2017).

Hopkin (2017) also states that risk management is a developing and evolving discipline and can improve the management of the core processes of an organization by ensuring that critical dependencies are analyzed, monitored, and reviewed. An essential function of risk management is its tools and techniques that will assist with managing the hazard risks, control risks, and opportunity risks that could impact these key dependencies. Another important thing is that "*risk management is not about controlling/mitigating risk out of existence. If business is to perform, management must learn to take more risks and to accept failure. To perform better than the rest, you must take greater risks, but it should be a calculated risk (the risk accepted is known, as is the likelihood and impact). It is not acceptable to take risks unwittingly – the past practice of silo-based approaches for managing pockets of risk leads to unclear responsibilities and a lack of visibility, thereby exposing the organization to unnecessary risk*." Aven (2020) states that risk management is a framework that covers all measures and activities

carried out to manage and govern risk while balancing developments and exploring opportunities on the one hand while avoiding losses, accidents, and disasters on the other. We can see a clear connection between risk management and risk since type A of knowledge relates to how this management is conducted.

In contrast, the B type of knowledge covers developing concepts, theories, approaches, and methods for conducting risk management. The cautionary and precautionary principles are essential in risk management and ensure that uncertainty is weighed in the decision-making process. Both robustness and resilience are cautionary thinking types and crucial factors in answering our topic question. The cautionary principle states that if the activity outcomes are essential and uncertain, cautionary measures should be implemented, or the activity should be avoided (Aven, 2019). As shown in figure 2 below, the risk management process is divided into five elements.

Figure 2

Five elements in risk management

(Horvath, 2021)

Many organizations carry out risk and vulnerability analyses every year. A ROS-analysis (translated from Norwegian) is a risk management tool that helps organizations identify and make visible risks for the organization. It assesses how undesirable events can occur, the probability that the event will occur, and what negative consequences they may have. ISO31000

is a risk management framework that will be clarified in chapter 3.4 and is an accepted standard. Risk management is relevant to answer our topic question regarding all the processes they include and theories that underline it. Both Perrow´s and Hollnagel´s theories are essential contributions when it comes to performing risk management. Their theories are fundamental in the design, execution, and evaluation process. Risk management is also relevant to improving robust and resilient systems that withstand cyber-attacks and keep personal and sensitive information safe.

3.1.5 Cyber-security framework (NIST)

Cyber-security risk affects a company´s bottom line, drives costs, and impacts revenue. The cyber-security framework was developed by the National Institute of Standards and Technology since the cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the US´s security, economy, and public safety and health at risk. They see similarities to financial and reputational risk. This paper presents a cybersecurity framework that focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risks as part of the organization´s risk management process. The framework is divided into three main categories: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references standard across critical infrastructure sectors, providing detailed guidance for developing individual and organizational Profiles. By using Profiles, the framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk (National Institute of Standards and Technology, 2014). The reason why we have chosen to only elaborate upon this framework is due to the importance this framework represents in the financial sector.

Cybersecurity contains risks, uncertainty, knowledge, vulnerability, and many other factors. When coping with cybersecurity in the financial sector, many measures could and should be taken to minimize risks against the organization and its public and private customers. Organizations tend to fulfill all requirements and protect their systems by having a good safety culture, working on cases related to risks, and following laws and regulations.

Developing into a secure organization gives a sense of security for both employees and customers. However, to achieve and maintain a secure organization when it comes to cyber security and digital attacks, some tools can help. In 2014, an article was published by the National Institute of Standards and Technology (NIST) entitled "framework for improving critical infrastructure cybersecurity." The framework provides a common language for internally and externally understanding, managing, and expressing cybersecurity risk. It can help identify and prioritize actions for reducing cybersecurity risk and is a tool for aligning policy, business, and technological approaches to managing this type of risk. The framework can be used to manage cybersecurity risk across entire organizations, or it can be focused on delivering critical services within an organization. The framework's core provides a set of activities to achieve specific cybersecurity outcomes and references examples of guidance to achieve those outcomes. It is not a checklist of actions to perform, but it presents vital cybersecurity outcomes identified by the industry as helpful in managing cybersecurity risks. The framework's core comprises four elements: function, categories, subcategories, and informative references (National Institute of Standards and Technology, 2014).

Figure 3

Framework Core Structure

(National Institute of Standards and Technology, 2014)

- ***Functions*** *organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.*
- ***Categories*** *are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."*
- ***Subcategories*** *further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."*
- I***nformative references*** *are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process* (NIST, 2014).

The five Framework Core Functions (National Institute of Standards and Technology, 2014) are defined below. They are not intended to form a serial path or lead to a static desire end state. Instead, these functions can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

- ***Identify*** *- Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business*

context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- ***Protect*** *- Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.*
- ***Detect*** *- Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.*
- ***Respond*** *- Develop and implement the appropriate activities to act regarding a detected cybersecurity event. The Respond Functions supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.*
- ***Recover*** *– Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recovery Function supports timely recovery to normal operation to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications* (NIST, 2014).

3.1.6 Complexity

Coping with complexity today is not a problem for process plant operators, hence the Three Mile Island (TMI) accident. However, complexity is for everyone and needs to be a focus point. While computers in 1981 were looked upon as the solution, they are now seen as the source of the problem. SRA Glossary (2018) defines *complexity* as ”*a casual chain with many intervening variables and feed-back loops that do not allow the understanding or prediction of the system´s behavior on the basis of each component´s behavior*.” Erik Hollnagel (2012) discusses in his paper why and how the meaning of “coping with complexity” has changed over the years and speculates on what may lie ahead. Hollnagel concludes that the classical mindset is that things go right. After all, systems are well designed and scrupulously maintained because procedures and training are complete and correct because people behave as they are expected to. They do what they have been taught to do because designers and analysts can foresee and prepare for every contingency. Coping is, therefore, a threat, and every effort should be made to minimize it or make it unnecessary. Increasing complexity has made modern technological systems intractable, hence underspecified. These are some reasons why we see this as something that needs to be investigated further, and it can be aligned with the NIST-framework and the ISO27001 standard.

3.1.7 ISO27001

The standards in ISO27000 include, in total, five standards. From ISO27000 to ISO27005. ISO27001 sets the standard for the establishment, implementation, maintenance, and improvement of a management system in informational safety (ISO27001 standard). This is the standard by which it can be certified, and the rest of ISO27000 is an elaboration and guidance concerning ISO27001. Because of this, it is why we consider this standard to be of importance. ISO27001 is a management system for information security that aims to protect confidentiality, integrity, and availability of information. By using this risk management process, the standard aims to trust different stakeholders with the knowledge that the risk is handled sufficiently and amply. If one looks at it from our point of view, this is a relevant and fascinating standard to investigate and elaborate upon. This approach will be seen as especially useful for organizations that implement the standard and for this thesis regarding respectably answering our research questions. When managing cyber-risks, the managers should take both the ISO27001 standard and The Personal Data Act into consideration. (Digdir b, n.d.)

3.1.8 The Personal Data Act

In 2018, the new Personal Data Act was passed and entered into force on 20 July 2018. The new law has been implemented through the EU Privacy Regulation in Norway and makes the Privacy Regulation Norwegian law. There have previously been laws on the handling of privacy, but EU Directive 95/46, the Privacy Directive, and the Personal Data Act from 2000. have now been repealed. The new law contains the Personal Data Act's rules on the laws and geographical scope (Kommunal- og distriktsdepartamentet, 2019). The geographical scope will not be discussed in this thesis.

Furthermore, the Ministry of Local Government and Regional Development (2019) states that the law specifies the right to carry out specific processing of personal data. A Norwegian age limit has been set for children's consent to process personal data using information society services. The Personal Data Act has also opened the door to lay down regulations on using unambiguous means of identification to transfer personal data to third countries. These were rules in the past, but not excellent and fixed enough. It provides better security regarding transfers and storage of personal information.

Chapter IV of the Regulation refers to general rules on data controllers and processors' responsibilities and obligations. They refer to Article 25, where the controller should use solutions with built-in privacy by implementing technical and organizational measures to ensure that the Regulation's requirements comply. The previous notification obligation for processing personal data according to the Personal Data Act 2000 has been replaced by other rules for the data controller and data processors. They are now required to document the processing of personal data, notify the supervisory authorities and the data subject in the event of a breach of personal data security, in addition to making assessments of privacy consequences and consulting with the supervisory authority before risky processing (Kommunal- og distriktsdepartamentet, 2019).

Through Article 30, data controllers and data processors are required to record, among other things, the purpose of the processing, categories of data subjects, and categories of personal data. They should also record any recipients of the information and categories of transfers of this information to third countries. This does not apply to companies with less than 250 employees that do not have the processing of personal data as their primary activity, in addition

to categories of processing that are not assumed to involve considerable risk. Data controllers and data processors are obliged to ensure adequate information security, with a view to Article 32, which significantly entails a continuation of previous rules. According to Articles 33 and 34, it is the duty to notify supervisory authorities and the data subject if it is probable that the breach will harm the data subject. The duty to notify is a new measure concerning the previous law (Kommunal- og distriktsdepartamentet, 2019). This section is truly relevant to our issues concerning privacy breaches and reporting following the law and regulations. We chose to involve the privacy information act and regulations because of the strong relevance to the topic question due to the management process in handling the risk of losing personal information. In the management process, it is almost impossible to withstand all sorts of accidents and attacks. Therefore, we find the NAT essential and should be part of this chapter.

3.1.9 Normal Accident Theory (NAT)

In 1984, Charles Perrow authored the book "Normal Accident Theory," which introduced a new way of thinking in the safety field. Perrow studied how accidents increase risk in high technological systems in this book. As mentioned earlier in the thesis, high technological systems are always complex. He claims that accidents will occur within these systems and are not something we can withstand. It is said that accidents will occur all the time, but at one time, an accident will occur. Perrow separates accidents from component failure accidents, which he refers to as when components in a system failure. The other type of characteristic he mentions is system accidents or normal accidents. This type of accident refers to when many components fail simultaneously, which makes the system fail, and an accident will occur. Both types of accidents are hard to predict, but a component failure accident is easier to detect. In contrast, a system accident is more difficult to detect since this type of accident can turn into an unknown progression. NAT can be useful when considering a security and safety perspective and be a factor in the three-factor model (Perrow, 1984).

Perrow (1984) has dedicated one chapter of his book to the complexity and refers to "complex interaction as generally those not intended not intended in the design." It is concise, clear, and understandable to describe such a big and challenging subject. A factor that plays a role in complexity is the size of a system and the number of diverse functions they serve. If a system is comprehensive, it can experience increasingly incomprehensible or unexpected interactions and become more vulnerable to unavoidable system accidents. Perrow describes an accident as "involving damage to subsystems or the system as a whole, stopping the intended output or

affecting it to the extent that it must be halted promptly." This definition is relevant to answering our problem. It points out that if an unwanted event occurs, either that a hacker enters the systems of organizations within the Norwegian financial sector or if an employee abuses his availability, a consequence may be that parts of the system fail or that the entire system goes down. This can lead to significant consequences, both financial, security and reputation.

To give an example where NAT has been a fundamental part of the scientific aftermath of an accident, we present you with the Three Mile Island accident, which has helped put this theory on the agenda.

3.1.10 Three Mile Island

On the 28th of March 1979, there was an accident at the Three Mile Island (TMI) Nuclear Generating Station. A partial meltdown of reactor 2 caused a small radiation leak. The accident did not cause any visible health effects for the workers, the public, or the environment, but the clean-up cost 1 billion dollars and took over one decade to clean up (Hopkins, 2001).

Many factors led to the event occurring, and this is where the NAT is relevant. TMI was a water-cooled nuclear reactor, and the water used in the steam turbines needed to be pure. Therefore, the external circuit contained a water purifier that needed regular maintenance, and this maintenance work triggered the accident sequence. The second part of the accident event was to overcome this danger, and the emergency pumps were supposed to come into action to maintain the flow of water in the external circuit. However, what happened, which is normal according to Perrow, is that several factors failed simultaneously. There was a leakage in a valve that set off a chain that caused the main pumps in the external circuit to shut down. The pumps had been blocked off two days earlier for maintenance, and the blocks had not been removed by mistake. This led to the pumps being inoperative, and the external circuit ceased removing heat from the internal circuit (Hopkins, 2001).

Hopkins claims that the failure of the external circuit would not have been critical if automatic safety devices in the internal circuit had functioned as intended. The automatic systems have done what they were supposed to so far, but the human actions were not performed according to the system's requirements. It can be seen here that human failure in the automated systems led to the incident being triggered. The reactor core began to overheat because the internal

cooling circuit started to overheat. It led to the reactor core shutting down as it was designed to do. The pressure in the internal circuit built up, and at a certain level, the relief valve of the circuit opened, as it was designed to do. The value malfunctioned, failed to close correctly and coolant continued to escape from the core. The system did what it was supposed to, and only human errors caused the accident (Hopkins, 2001).

The system's design was in such a way that the lights on the control panel indicated that the valve had closed even though it was open. Even though there was a light, the operators did not know they were experiencing a loss of coolant. It led to an ongoing loss of coolant, and the pressure in the internal circuit dropped to a level that meant that it would be unable to continue conducting heat away from the core. Another safety device kicked in and forced the high-pressure injection pumps on, forcing additional water into the internal circuit to compensate for the loss of coolant (Hopkins, 2001).

3.1.11 Redundancy

A theory called High-Reliability Organizations (HRO) takes a standpoint that accidents in high technology systems can be prevented, and it is possible to have a reliant system that is based on unreliable components (Aven et al., 2004). This theory investigates how organizations can coordinate to achieve high performance where a mistake or fault can have profound consequences. In this thesis, we have chosen redundancy as a topic that may provide answers to our questions and discussion.

Redundance can be seen in both a structural and cultural way. While the structural dimension focuses on the development of competence and communication, the cultural dimension looks at the culture of, for example, cheering information and reporting errors (Rosness et al., 2004). With redundancy being a crucial part of an HRO, redundancy is a key element when dealing with multi-layer security. It concerns the complexity and competence of personnel involved or an overlapping function in a system. This means that if a function is failing, there is someone else capable of stepping in, or a component takes over for the failing function (LaPorte & Consolini, 1991). Moreover, we think this is important to our thesis and aim to elaborate on redundancies and resilience in our discussions.

3.2 Summary of theories

In this chapter, an essential theory is accounted for. To answer the topic question, we will use more than one theory. The different theories will come together to answer both the topic question and the sub-questions. Concepts connected with the science of risk will be used in discussion with the framework and standard used by the sector to understand how the risk of losing personal information affects the understanding and approach to cyber-risk. While this thesis analyses scientific documents, we aim to present the reader with the most vital information to understand the underlying goal.

Perrow's theory on NAT connected with complexity, redundancy, the NIST-framework, and the ISO standard will be tightly linked in the discussion part of this thesis. Various aspects of the theories will be discussed because they all contribute to different insights into the questions at hand. Significantly, the focus on complexity will contribute to sufficiently answering the questions.

4. Methods

We want to provide an overview of our different choices regarding methodology to explain how the Norwegian finance sector handles the risk of losing personal information. In this chapter, we present the rationale behind our methodological choices and explain the process for analysing our collected data. Further on, we will explain how this data collection is structured. Lastly, the reflection will be provided to elaborate upon the strengths and weaknesses of our research.

4.1 Methodological approach

The research design used in this thesis is a content analysis that follows an abductive approach. An abductive design is a place between induction and deduction. An abductive approach addresses weaknesses associated with deductive and inductive approaches (Dudovskiy, 2016). As illustrated below in figure 4, induction will be connected to qualitative methods by interpreting empirical, while deduction seeks to confirm existing theories and hypotheses (Skjelvik, 2019). This coincides with a quantitative method. Tjora (2021) states that abduction is a set-by-set deductive-inductive method that continuously works on building bridges between induction and deduction. We chose this approach because we want the empirical and theory to

contribute to answering the topic question as abduction is used to explain and understand a broader range of contexts for how companies protect themselves. We wanted the thesis to be as open as possible to let the collected data lead our research.

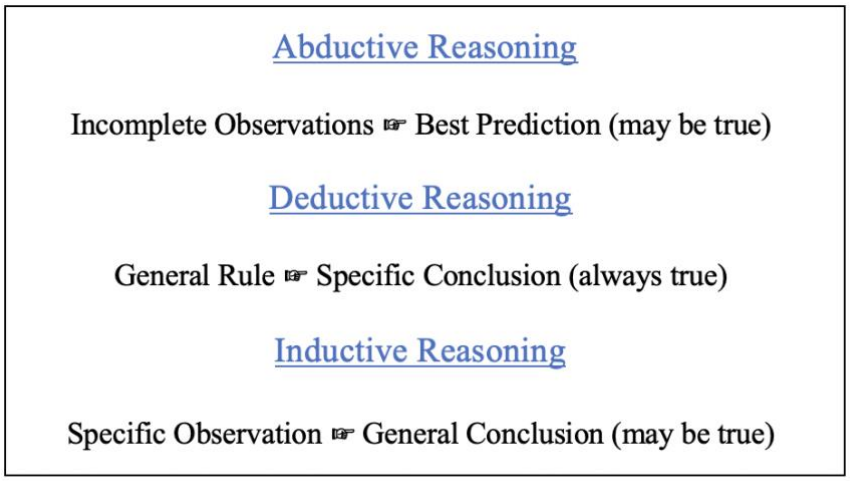

Figure 4

Methodological overview

(Bradford & Weisberger, 2021)

In this thesis, we have chosen to use a qualitative approach to create an understanding of the topic question. Qualitative means what has to do with someone's or something's characteristics or qualities, as opposed to what has to do with numbers (quantitative) (Malt & Tjernshaugen, 2020). We have searched documents and articles to collect data and understand the subject well.

Furthermore, the research strategy in this thesis will consist of a content analysis performed using a literature review and document analysis. This means that we detect details, describe different tools, and look at the structure in the text to say which function these parts and tools have (Ridderstrøm, 2021). A literature review is a search and evaluation of the available literature on a given subject or chosen topic area (Royal Literary Fund, 2022). In more considerable written work, such as a dissertation or project, literature research is often one of the first tasks after identifying a topic. Reading combined with critical analysis can help refine

themes and formulate research questions. A literature review builds familiarity and understanding of current research in a particular field before undertaking a further investigation. A literature review should enable one to find out what research has been done and identify what is unknown on the topic (University of Edinburgh, 2022). Document analysis is a systematic procedure for reviewing or evaluating documents in both electronic and printed material. In qualitative research, document analysis requires that data be examined and interpreted to elicit meaning, gain understanding and develop empirical knowledge (Bowen, 2009). This is what we aim to do in this thesis. By doing so, we know that the research in this thesis could be enhanced by performing interviews. However, with the sensitivity of the topic and the questions we aim to answer, we chose to proceed without interviews. Another reason is that we want the thesis not to be colored by other people´s opinions.

4.2 Data collection

Throughout the literature analysis, we have collected relevant documents and articles that have laid this thesis's foundation. There has been a widespread collection of data, and all the data is publicly available. This data collection includes the framework, standards, laws and regulations, and relevant cyber-security documents and articles. By analyzing the documents, we aim to use them to understand better how the Norwegian financial sector can improve on the risk of losing personal information and dig deeper into the theoretical understanding of the thesis. For example, the NIST-framework and ISO27001 standard have been the subject of an in-depth analysis. In this thesis, they are used to see how the Norwegian financial sector works with cyber security in a preventive phase, at the same time as they help guide companies if breaches occur. Additionally, we aim to look at the framework and standard critically and provide input where we recognize weaknesses and make suggestions for improvement. We aim to provide insight on this in chapter 5.

	Publisher	Year	Function
NIST Framework	US National Institute of Standards and Technology	2018	A set of industry standards and best practices to help organizations manage cybersecurity risks.
ISO27001	European Committee for Standardization	2017	Help organizations establish, implement, operate, monitor, view, maintain and continually improve Information Security Management System.

Table 2

Overview of NIST-Framework and ISO27001

Two of the most influential documents used in this thesis are displayed above. This is to clarify and enhance the reliability of the thesis. Table 2 shows us who the publisher is, which year it was published, and the intended function they yield. Today, it has become easier to search within large documents. We have searched for relevant words regarding cyber, threat, complexity, and uncertainty using a simple word search. In some of the documents, we have used the word search to figure out how much the author has emphasized different concepts and to make it easier to find the relevant information for answering the research question in our thesis. After discussing the relevance of each document, we have included what we believe is most important to answer the topic question in the best viable way.

Furthermore, an essential part of this thesis is to use the terms “describe” and “evaluate.” These terms are essential and give us a general understanding of how to answer our questions. Johannessen, Tufte, and Christoffersen (2018) claim that this type of research is both substantiating and documenting. These terms are then used to set out features or characteristics and to make judgments based on evidence in analyzing the information we have gathered. We use the term “describe” along with other terms with the same type of meaning. For example, explain and illustrate. “Evaluation” is mentioned in relation to, for example, elaboration and discussion.

4.3 Data generation

The financial sector involves a lot of diverse types of activities that are influenced by risk. This might include transactions, payment systems, physical money, and personal information activities. In this thesis, we have chosen to investigate further the risk of losing personal

information. Therefore, we base our theoretical, analytical, and methodological investigations on documents that focus on this accurate and specific topic. Considering the decision not to use key informants in an interview situation, it has been essential to find and analyze documents that have been a contributing factor in shaping the thesis and providing relevant information that gives us a good understanding that can be used further in chapter 5 and in our discussion. We intend to make a qualitative analysis of the problem at hand to judge how the Norwegian financial sector handles the risk of losing personal information. Previous research mentioned in chapter 1, documents, and articles from the field of science is then seen concerning the different theories and our research question. Our sources include framework, standard, and laws.

4.4 Criteria

Reliability and validity are research techniques used to assess the accuracy of measurements. Reliability refers to the stability of a measurement scale. In other words, how far it will give the same results in separate locations can be assessed in diverse ways. These can be stability, internal consistency, and equivalence. On the other hand, validity is the degree to which a scale measures what it is intended to. Reliability is a statistical measure of how reproducible the instrument's data are and can be equated with stability, consistency, and dependability. Validity can be said to be in line with the meaning and interpretation of a scale. Validity is not absolute, but it is a matter of degree rather than an "all or nothing" concept (Bannigan & Watson, 2009).

Tjora (2021) writes that it can be both an advantage and a weakness to have a personal commitment to the topic you are writing about, something we see as an advantage. During our study time, we have not had subjects that have dealt explicitly with cyber security but have had subjects that have given us a sound basis for understanding how the sector can handle attacks against privacy. Although we have not had subjects that specifically deal with cyber, our interest in the subject has grown with our time in the study. None of us work or have previously worked in the sector, which gives us an objective view of the topic. This helps to increase the reliability of the thesis. Since we started authoring the thesis, we have had some hypotheses we have been conscious of. However, these hypotheses have not omitted documents that have been relevant to the thesis, even though they have been "contrary" to our hypotheses. What we have done has a degree of reliability, and we justify this since the documents we have analyzed have either

been public, peer-reviewed, scientific, or critical. Our thesis is built around professionally robust theories and documents that give the thesis higher reliability.

Based on how we have built up the task and what methods we have used, it can be said that we have gained access to the most necessary documents that are available. As mentioned, we have used valuable documents and analyzed them in a way that has been satisfactory for the thesis. That helps answer the research questions, which can answer our topic question. Our task cannot be utterly valid because we have not been given access to documents that the various organizations in the sector use in their work regarding cyber security and personal information. It is difficult for organizations to give us access to these types of documents, given all the internal procedures organizations have, which could make them more vulnerable if they are published. The task would have been more reliable and valid by accessing and using this type of data.

4.5 Strength and weaknesses

Due to the character of the topic question in this thesis, we have chosen not to do any interviews. Initially, in this thesis's beginning and planning stage, we were aiming to perform interviews. However, due to the nature of the questions and the cyber security environment, we found it challenging to find informants who wanted to help us with this type of issue. It may seem that the informants do not want to reveal strategic measures in this type of question. The informants seem to want to keep the cards close to the chest. This made us think in another way, and we decided to go away from interviewing informants and advance to a structured, analytical, informatic thesis to answer our questions.

This study is based on documents that are publicly available. The documents we have analyzed give the thesis reliability. If we had informants, this could have strengthened our material and data, giving the thesis more credibility and validity. Furthermore, basing the thesis on available public documents has allowed us to analyze the risk of losing personal information. This has given the thesis a substantial amount of information to analyze and could be one of the greatest strengths of this thesis. Although, analyzing the publicly available documents provides us with a limited selection of information. Given the circumstances that we do not perform any interviews, this has allowed us to dig deeper into the material. Moreover, the fact that we do

not have input from experts in an interview situation gives us credibility because we can proceed with the qualitative material without any interference and different views on the questions.

This thesis engages in the theoretical and empirical areas in the analysis without any interference from informants, which creates strength in this study. With this in mind, it is time to leap over to the empirical part of the thesis.

5. Empirical

Moving back to the beginning, we acknowledge significant developments regarding cyber-attacks in the Norwegian financial sector. Finanstilsynet made an overview of the development in attacks against Norwegian organizations and will be presented in chapter 5.1.1. The financial sector is within critical infrastructure and the importance of maintaining essential societal functions. The importance of dealing with this type of attack has been highlighted through the development of the GDPR, where the latest version was published in 2018. In the introduction, we present different attitudes on risk, and we take Aven and Renn's theories as our starting point that risk must be based on uncertainty instead of probability. We choose this direction regarding risk since systems in the Norwegian financial sector are complex and contain a great deal of uncertainty. It is not because the systems are insufficient that it creates insecurity, but because of the complexity of the users involved. This can also be seen in the example of Three Mile Island, where Perrow highlighted the NAT and set the tone for parts of chapter 5.

The documents used in this chapter are from reliable publishers and authors and are currently the most used and acknowledged framework and standard within the cyber-domain. See table 2. They are well formulated, include the most vital processes in cyber-risk, and can be used as a recipe. It is not only used as a recipe in the financial sector but also translated into other sectors, e.g., the health sector. In addition, other articles presented in this thesis are either peer-reviewed or based on scientific knowledge. For a better set scene, we also choose to include, for example, newspaper articles to show the importance of the topic. For more detailed information, we refer to chapter 4.

In the introduction, we presented type A and B knowledge, and we will further use these with a specific approach aimed at B knowledge to refresh our minds. This type of knowledge is based on concepts, theories, frameworks, approaches, principles, methods, and models. We chose to look at this type of knowledge because it is aimed at our thesis's problem. This part of knowledge conceptualizes and understands risk, which is vital for the task and the problem at hand.

The importance of the problem that will be answered in the thesis is made visible in Chapter 2. Norway is calculated as the third-largest digitized country globally based on the DESI-index. Even though Norway is in third place in this award, this does not mean that Norway is third best when it comes to handling digital threats. We see this in PST's annual threat assessments of the situation in Norway, where we still have many obstacles to overcome to be resilient, robust, and redundant.

Although the financial sector constantly deals with uncertainty and complexity, it cannot withstand all attacks. As Perrow (1984) mentions, it is not always the case that there will be an unexpected event with severe consequences, but the probability is high that it will happen at some point. This reflects how we have formulated the problem and our research questions reasonably.

Drawing on cyber-attacks, how is the risk of losing personal information handled by Norwegian financial sector?

We will answer this topic question with three sub-questions. We believe our topic question is highly relevant due to digital development today and the dangers cyber entails. The methods used today by the actors implicate not only the companies but also the users and customers. This means that companies should focus on their internal security routines but also on the users and the security that is provided to protect the user's personal information. As presented in attachment 2, several methods can be used to obtain sensitive information. *Phishing* is a prevalent method intended to collect access to information through the user.

Furthermore, we use information and data that have been presented in chapter 4 to answer our questions. This is based on information we collected during this period of authoring the thesis. The theories that have been presented in chapter 3 are peer-reviewed books and articles. These theories will, in this chapter, be used to draw lines between the practical and the theoretical

approach to our research questions, where the practical part is to see how the industry uses the theory and where they are, while the theoretical part of the case more on the actual discussion of the issues. However, articles found on the internet will also be used to set the scene and context for the thesis.

Our sub-questions contribute to answering our research question. Additionally, the chapter will be structured like our sub-questions in chapter one is presented. We see this to be fruitful, even though there is no clear line between our subjects. Some of our headlines may seem to overlap, which may be correct. For example, actors will be presented in separate ways in both chapters 5.1 and 5.3.

This introduction sets the stage, and it is time to introduce the empirical presentation of the first sub-question of the thesis.

5.1 How does continuous change of cyber-attack influence risk description in the financial sector?

We have introduced our topic question. We start with this essential first sub-question to provide a general overview of the development of cyber-attacks in the Norwegian financial sector. To understand how these attacks influence the risk description in the financial sector, we are obligated to provide information on the development of cyber-attacks and who the actors who execute the attacks are. Our three sub-questions must be elaborated upon to complete and understand the importance of handling lost sensitive information.

Furthermore, we aim to present different methods used by the actors. This will provide a better understanding of the overall threat picture. Two examples of accidents will be presented, where we intend to look at different events. The first example is from Østre Toten municipality in Norway. This example indicates how a cyber-attack might affect society when it occurs and explains the risk description in cyber in an analytical context. The TFM will contribute to the analytical context. We will explain how complex systems are challenging to operate when unwanted events occur. We will see this example considering Charles Perrow´s and Erik Hollnagel´s theories concerning NAT and complex systems.

5.1.1 Development in cyber-attacks

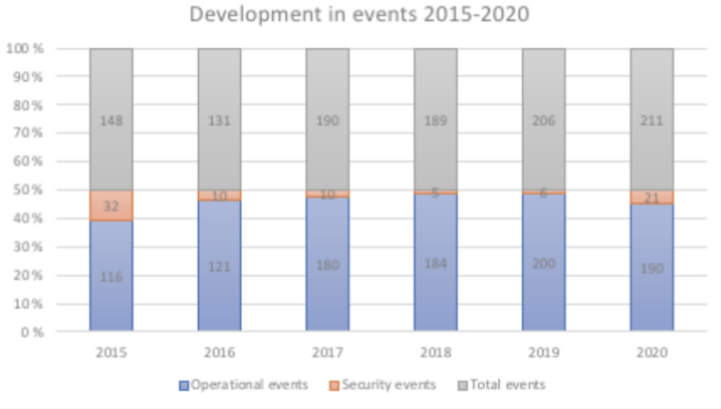

Figure 4: Development in events

(Finanstilsynet, 2021)

National reports on risk and threats in Norway could be argued to be on a more comprehensive agreement, but it is a bit vague in the financial sector. In December 2009, it was decided through the new ICT regulation that institutions should report cyber events to create an overview of threats to the sector (Bellamy & Berg, 2019). In figure 4, we illustrate Finanstilsynets' overview of reported events. The figure is based on Finanstilsynets risk- and vulnerability analysis from 2021 (Finanstilsynet, 2021). However, the figure does not reflect how the cyber-attack change has evolved over the years.

Figure 4 shows that there were more events in 2020 than in 2019, and we can also acknowledge the vast difference in actual events from 2015 to 2020. However, more events considering security in 2020 than in 2019 were reported. In 2020, 21 security events were reported out of 211, which translates into about 10%. Furthermore, there is a clear evolution from 2015-to 2020, although 2016 and 2018 are the only years with declining stats compared to 2015 and 2017. Most security events evolve into digital crime- ten of the events reported in 2020 concern a DDoS attack (see attachment 2) (Finanstilsynet, 2021).

Additionally, in 2020 two different varieties of infected malware was reported (Finanstilsynet, 2021). One of the incidents was the Østre Toten case, as described below. This figure indicates that the trend of total events is increasing every year, and we can assume that the trend will continue developing in an increasing direction. However, the figure does not consider how the actual methodology of the attacks has changed.

Operational events: Reports from financial institutions, like banks, are primarily about events that deal with errors connected to failure in different services. One example could be the failure to complete the payment service. The events that got the most attention in 2020 were DNB events that caused several days of delay in salary payment and holiday pay to many customers (Finanstilsynet, 2021).

Furthermore, most of the vulnerabilities connected to this analysis from Finanstilsynet point out vulnerabilities in operational events, cyber-crime, confidential information, and access control with the intention of areas that must be continually strengthened. In this analysis, it is also stated that complexity in technical infrastructure is increasing and that there are challenges connected to innovative technologies (Finanstilsynet, 2021). This is remarkably interesting to this thesis because we need to look at the trends and the development of cyber-attacks to comprehend how this influences the risk description in the financial sector. Complexity in technology is mentioned in the analysis, and the sector needs to be on its toes when developing security events.

There have been several changes in the way hackers attack in the last few years. These changes include the method used to attack and the intention of the attacks, for example, to steal personal information or other information like the attack on the Norwegian Storting in 2020. These changes are forced by the complexity of both attacks and the systems used to prevent them. NSM claims that "complexity is the biggest vulnerability in the Norwegian digital society today" (NSM, 2018). In this report from 2018, NSM also mentions that this complicates the management of the event and that it might be harder to detect. Digitalization and technology both work in tandem as a growing trend, and it is expected that different actors (see 5.1.2), like hackers and other criminals, will be able to use digital technology to develop new and more effective methods to penetrate their targets (NSM, 2018).

"Advanced actors have comprehensive resources available, and if the goal is important enough, they will find a way in" (NSM, 2021). The accelerating trend of digital breaches will be expected to accelerate further, claims NSM. For example, mapping and successful information gathering against Norwegian goals will continue (NSM, 2018).

5.1.2 Actors

As mentioned in the previous chapter, there has been a notable change in cyberattacks, reflecting the actors who carry out the attacks. The report from NSM (2021) refers to two diverse types of threat actors, state, and criminal actors, who try to exploit vulnerabilities in functions, businesses, and systems by using a wide range of digital tools. Over the past two years, the threat actors have adapted to the situation caused by covid-19, exploiting the systems' weaknesses. The actors use more methods today than before to pressure to get ransom paid, where the publication of sensitive data is one of them. Therefore, these conditions provide a change of pace.

Both state and criminal actors have the intention and capacity to carry out cyberattacks on Norwegian companies and interests. The Russian and Chinese intelligence services are the most active actors based on the Norwegian State and Social Security (FCKS) assessment. Two large nations have advanced tools and methods available and can operate on a resource and capacity investment in the domain. They can operate within Norwegian infrastructure over time and simultaneously observe large and complex operations towards several targets across sectors. In the past, NCSC has seen trends where actors observed individual operations towards one goal to a greater extent. Here, too, one sees the change in cyber-attacks (NSM, 2021).

The actors have different goals for the attacks they carry out. It can vary from intelligence, sensitive information, and money. NSM points out that some actors, on the other hand, want a lasting foothold in Norwegian companies where the purpose is to extract information that can be of intelligence value, both in the short and long term. No findings have been made against the Norwegian financial sector but against the research and education sector, the central administration, and the defense sector (NSM, 2021).

The methods used vary from actor to actor and may, in several cases, have significant similarities. In recent years, phishing has become a standard method, where the actor sends an email to get the recipient to open a malicious attachment or link. It is a method that has been used over time, but NCSC is regularly contacted by companies that experience such attacks. This can be both towards the business and towards the customers. This attack is often admirably adapted to each target, and the threat actors use publicly available information to tailor emails

before being sent (NSM, 2021). Therefore, companies should be careful about how much information should be available concerning integrity, confidentiality, and accessibility (GDPR).

Only when an actor gains a foothold in a company or individual first gains access to their goal. The access can enable the actor to install the malware in the systems, add "back doors," and further extract data from the company. The type of malware and tools the actors use in the various attacks varies. NSM divides it into two categories: one is so-called "off-the-shelf products" available on the internet. Advanced actors specifically develop the other types. To disguise the malicious act as legitimate, actors often use administration tools to accomplish their goals. This can make detection and attribution difficult. In most cases, a combination of these two is used (NSM, 2021).

In some attacks, the actor is looking for a ransom and can prevent companies from using their IT systems through viruses. In this way, the companies can be pressured to pay the actors so that they will be able to maintain ordinary operations. At an international level, it is reported about different methods the actors use for this type of extortion. Four methods are central-encryption, publishing, harassment, and denial of service (RDDoS) attacks (see attachment 2). What the four methods have in common is ransom. The threat actor will require money to decrypt the business's systems regarding encryption. This has already been mentioned above. If the actor uses publication as a means of pressure, the company will be threatened with the publication of data obtained from the company. In harassment, the actor may pressure or harass the company's customers or stakeholders. This can affect the business's reputation, something they do not want. The latest means of pressure is the denial of service, where the actor can expose the company to a denial of service with a claim for ransom. NSM points out that during 2022 there is a remarkably considerable risk that more Norwegian companies will be exposed to ransomware viruses, which could lead to extensive consequences. Even if companies pay a ransom, there is no guarantee that they will get the data back (NSM, 2021).

In January 2021, Østre Toten municipality was exposed to an encryption virus with ransom demands. It was a ransomware virus with malware PYSA. The consequence was that the entire virtual server package for the municipality was encrypted and locked down. In addition, the Internet-based backups were encrypted and made inaccessible. The actors also stole a significant amount of data, and double extortion was considered possible. This led to the municipality's operational capacity being severely weakened and the situation worsening on

March 29, when PYSA published parts of the data stolen on the dark web. Østre Toten municipality had to handle sensitive personal information astray, at the same time as they had to inform and support the affected people. At NSM's annual security conference, the mayor of the vulnerable municipality spoke. One of the measures implemented in the municipality was that the elderly's alarm systems in nursing homes were replaced with bells, the locking system for the municipality's buildings was out of order, and the health station for children and young people's medical records were no longer available. They had to operate manual systems without functioning IT systems for several months. This example shows that it is not only the system itself that can have consequences from an attack but also large sections of the population. Many businesses affected by a ransomware virus are unprepared for this to happen to them (NSM, 2021).

In 2020 and 2021, the National Cyber Security Center (NCSC) in NSM experienced significant growth in activity level in the digital space compared with previous years. This trend is also presented in the previous chapter. The number of serious incidents registered with NCSC in 2020 was three times as many as in 2019. This shows a marked increase. In many of these operations, several companies were affected and, in some cases, had branches of international operations. In this report, both the E-service and PST have pointed out that the foreign intelligence and influence sector remains a significant threat to Norway and our interests (NSM, 2021).

For threat actors, the digital space is an arena for interaction and information exchange across citizens, businesses, sectors, and countries. It provides an opportunity for foreign states to influence operations and the dissemination of misinformation, which can create uncertainty. It can also help create discord, undermine trust, and influence public discourse. Today we are facing a change of pace within the digital risk picture in Norway. Some actors continuously carry out operations towards Norwegian targets, where our most important values are managed. The attack on the Storting shows the severity of the national risk picture (NSM, 2021).

There is significant variation in how the attacks take place, and the attack type depends on what the player is trying to gain. See attachment 2 for more information regarding different types of attacks.

5.1.3 Risk description to cyber

We introduced the definition of risk at the beginning of the theses. Together with the expert committee of the Society for Risk Analysis (Aven, 2020), we agree that it is impossible to agree on one unified definition of risk. In this context of cyber risk, we acknowledge that we need some explanation. When dealing with cyber risk, we sometimes speak about the attacks that cause harm. In our case, we can say that it is about the threat and uncertainty. We choose to define the threat, based on Oladimeji (2006) and Aven (2020), that a cyber threat might be seen as "a potential violation, where the intention is to initiate an attack on the security of a system, with the intention to inflict harm, fear, and access, where the event may have negative impacts." The reason we choose to, in our view, improve on the definition is because we acknowledge the scientific gap between the expert's definition of risk, along with the difficulties in agreeing upon one set definition, and the threat definition when it comes to "cyber-risk." There is a gap between the risk and cyber-risk because of the different angles of approaches.

In chapter 3.2, we described the TFM and its importance. We argue this model to be highly relevant to understanding the influence on risk description in cyber-risk. This model is essential because of the influence of cyber-risk threats, values, and vulnerabilities. Furthermore, we need to elaborate on the complexity of risk and the safety dimension, which means that the TFM can help us understand.

First, we have the importance of values in the Norwegian financial sector. Engen et al. (2016) claim that the TFM could be used in risk analysis when handling risk. We agree with this statement. In our case, financial sector values could be information, money, and access. The constant change in the threat picture effectively suits this thesis because of the many different possibilities the actors have when carrying out an attack and the balance between them. This balance is vital when we elaborate on the risk description because of the many threats and the vulnerability. As mentioned in chapter 3, the threat could be seen concerning actors with a severe focus on complexity. In complexity, there is a factor that plays a significant role in the size of the system. If a system is massive and complex, it can lead to unexpected interactions and might become vulnerable to system accidents. With this in mind, threat and complexity might influence risk description. In the third part of the TFM, we find the vulnerability. Both value and threat could lead to vulnerability, so this is easily connectable to cyber-risk. Complex systems with an advanced threat picture and tightly linked systems might make us vulnerable

due to the new environments and constant change of new risk descriptions (NOU 2000: 24). The reason TFM is meaningful and suitable for cyber-security is precise because of the many diverse types of factors that are involved in cyber-risk.

The connection between value, threat, and vulnerability is crucial in the risk description and the importance of robustness, resilience, and redundancy. Boholm et al. (2016) claim that a security perspective influences threat when it has the potential to harm important values and has, therefore, a potential to influence risk description. Resilience and redundancy play such a role because they influence vulnerability and threats. A robust and complex system could be argued to have less vulnerability that could help lower the threat and the security level.

Regarding risk management, with the above statements, could a vulnerability analysis include a more comprehensive focus on complexity in line with Perrow and Hollnagel's theories regarding the field of complexity and human factors? We acknowledge that there might be some flaws in the current risk description.

5.1.4 Human factors

Based on the theories of Charles Perrow and Erik Hollnagel, chapter 3 introduced how complex systems increase the likelihood of risk. It is not the case that there will always be an unexpected event with severe consequences, but the probability is high that it will happen at one time or another (Perrow, 1984). Charles Perrow has received mixed feedback on his normal accident theory, but he shows his theory with an example from the USA. The systems that the Norwegian financial sector uses today are more complex than ever, and it is a sector that should keep up with the development of its digital platform.

On the 28th of March 1979, there was an accident at the Three Mile Island Nuclear Generating Station. The accident did not cause any visible health effects for the workers, the public, or the environment, but the clean-up cost 1 billion dollars (about $3 per person in the US) and took over one decade to clean up. (Hopkins, 2001). Many factors led to the event, which is where NAT is relevant. However, this section is not about the TMI accident but is to illustrate NAT in a context with clear lines to the Norwegian financial sector and our questions.

It is possible to link this example to the financial sector, how the risk is acknowledged and how a possible accident or a threat can be recognized concerning the risk description. As LaPorte and Consolini (1991) claim, there needs to be a capable person or system that takes charge when something in the system fails. If an actor gains access to a system in one way or another, the system needs to be as redundant, robust, and resilient as possible. Since the systems today are so complex, the people monitoring the system may find it challenging and confusing to understand what to do if a system breaks down or an attack occurs. This is something we need to be aware of, and seeing this accident at TMI, this is something we can translate to the Norwegian financial sector. It needs to be an essential and highlighted part of the risk description and how it will influence the work on cyber security.

With that, we need to acknowledge the importance of the human factor in a system. Human error is commonly used to explain the causes of accidents and relates to planned and unplanned actions. This aspect suggests, among other things, that different systems would have fared better if it were not for the unruly behavior of people monitoring the systems. Human error often comes unexpectedly and is commonly used to explain that accidents happen in high-risk systems, advanced systems, and critical infrastructure (Engen et al., 2016). It could be said that human error can explain 80-90% of accidents occurring in high-risk systems. As Reason (1997) claims, this number is a reliable estimate when there are humans involved in monitoring the systems. However, these estimates do not explain why accidents occur. Reason (1997) defines *human error* as "the failure of planned actions to achieve their desire ends- without the intervention of some unforeseeable event."

Even though human error often explains how accidents occur, it is essential to remember that this is not an explanation. NAT explained in chapter 3.4 shows that it is expected that accidents involving humans may occur at one time or another. In Perrow´s book regarding NAT, he dedicates a chapter to complexity. We acknowledge the complexity and human error as a significant part of a high-risk system and the vast number of functions they serve. We find it essential that these factors be included in a more significant way in how the risk description influences the financial sector regarding cyber-risk.

In this chapter, we have given an empirical overview of how the change in cyber-events has developed over the last seven years and how the involvement of actors may interact with these changes. Furthermore, we have made a visible risk description to cyber risk using the TFM and

explained how the NAT, with its human factor and complexity, plays a significant role in influencing risk description in the financial sector.

5.2 How does risk management handle increased systemic complexity?

It is time to feast our eyes on the second sub-question about how risk management in the financial sector handles increased systemic complexity. Firstly, we aim to present an overall picture of risk management, focusing on the current ISO standard and the framework used to handle cyber-threats. This will contribute to an enhanced understanding of how the sector handles the problematic aspect of complexity. Furthermore, we will use an analytical context to explain systemic complexity to understand better how the sector currently handles complex cyber-risk. Vulnerability and uncertainty play a vital role because of the constant development of the threat picture and complexity within the systems. We find it necessary to acknowledge both uncertainty and vulnerability in complex systems. The complexity within the systems itself might contribute to unintended events and therefore contain systemic risk.

5.2.1 Risk management

The importance of risk management is no doubt crucial to the financial sector when it comes to managing constant changes in threats and maintaining a robust system (Brown, 2021). Hopkin (2017) states that risk management is a developing and evolving discipline and can improve the management of the core processes of an organization. It is done by ensuring that critical dependencies are analysed, monitored, and reviewed. It is important to remember that risk management does not have the same meaning in every situation. Different situations can have different outcomes and risks, therefore, should be managed individually.

When managing cyber-risk, it is essential to have the risk management process in mind. Implementing the correct and necessary processes to handle systemic risk is vital. There is widespread confusion about the causes and the definition of systemic risk, and how to control it. Scholars tend to think that systemic risk primarily involves financial institutions such as banks (Schwarcz, 2008). However, the CFA Institute refers to systemic risk as a breakdown of an entire system rather than simply the failure of individual parts. Policymakers need to limit the build-up of systemic risk and contain economic crisis events when they do happen (CFA Institute, 2022). Systemic risk is then transformable to the Norwegian financial sector in this thesis regarding their position in society and their vulnerability concerning cyber-threats.

The first step in a vital risk management process should be to identify the current risk picture and future risks. This might include regulatory and strategic risks, and it is crucial to identify all the potential types of risks that the sector may face. If all the possible risks for the sector have been identified, the risk analysis, which is the second step, should answer some of the following concerns. What is the likelihood of these risks occurring, and what will the consequences be for the sector? By analysing risk, the sector can create its response depending on the risk severity. It is fruitful to understand the link between the risk and the aspect of the field (Brown, 2021). The higher the risk is toward the field of cyber threats, the higher the risk is to the sector. The next step in the risk management process is after completing a comprehensive and detailed analysis of risks. It is essential to rank the risks in order of severity and then make the correct prioritization. However, it may be challenging to agree upon and foresee the impact the threats may have on the sector or on a system with an organization (Brown, 2021). Again, this is because of the constant change in methods used by different actors and the threat picture. As Danske Bank says, "we acknowledge the frauds are becoming better and better, the risk picture is changing, methods used are changing, and this leads to higher risk." (Marthinussen, 2022).

Once risks have been analysed and prioritized, it comes down to action. Every risk needs to be eliminated or contained. If this is done manually, members of the team or system need to act. This could enhance the risk of failure due to the enrolment of humans and the human factor (Brown, 2021). We acknowledge that the human factor is mentioned in this section and find this appropriate. However, even though it is mentioned, there is no actual statement on how this could be handled. Could it be that there should be some information on how to handle human interference in complex systems?

Furthermore, the five Framework Core Functions (NIST 2014), has seen risk management from the operational point of view. Five steps which include:

- Identifying
- Protect
- Detect
- Respond
- Recover

This is in correlation with Brown's suggestions on how risk management in cybersecurity should be carried out sufficiently. We find that this is something that the section also works after regarding risk management. However, even though we agree upon the specific steps in the management part, we acknowledge that there are parts in the process that lack definitions and the acknowledgment of complexity and uncertainty. For example, in the five steps from the NIST 2014, there is no mention of either complexity or uncertainty. In the process of Protection, it says, "...the ability to limit or contain the impact of a potential cybersecurity event." We agree, but then again, it is acceptable that the system at hand could limit the threat and contain the impact of an attack. However, there needs to be more focus on complexity and how uncertainty impacts the system's ability to protect and contain a threat.

The cyber-security framework presented by NIST gives organizations a clear understanding of how to comprehend how they should prioritize when handling cyber-threats. NIST´s framework presents a cybersecurity framework that focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization´s risk management process. The framework is presented in detail in their document, but we have chosen to focus on the framework core structure. In chapter 3, we explained the framework core structure in a detailed manner and all its functions. It is helpful for the Norwegian financial sector to have a detailed and precise framework for its cyber-security work. We acknowledge the lines between risk management and NIST´s cyber-security framework. Both are risk management methods angled toward improving the handling of cyber events. However, we argue that it could be fruitful to incorporate the side effects of complex systems used within the sector.

Could it be that the ISO27001 standard used in risk management as a broad recipe in the sector is more “fine-tuned” when handling systemic complexity? It is time to look at the ISO27001 standard that is currently used broadly by the sector.

5.2.2 ISO27001

One of the many tools risk managers can use when handling cyber-risk is the ISO27001 standard. The standard has a set of demands for establishing, implementing, maintaining, and continuously improving management systems in cyber-security. The development of digitalization plays a significant role in this standard. Establishing and implementing a

management system for cyber-security within an organization will always be affected by its needs and goals, security demands, size, and structure. The management system for cyber-security keeps the confidentiality, integrity, and accessibility to information by using a risk management process that gives stakeholders and customers trust since the organization appropriately manages the risks. Integrating the ISO27001 standard within an organization's process is essential since cyber-security should be considered by the design of the process, information systems, and security measures (Standard Norge, 2022). This standard is an essential management system for cyber-security.

The ISO27001 standard is essential when coping with systemic complexity in risk management. Since it is an international standard, there is a widespread understanding and agreement on handling cyber-security. Norway is one of the many countries that have developed this standard, and many organizations use it. The standard states that "the extent of documented information for an information security management system can differ from one organization to another due to: the complexity of processes and their integrations; and the competence of persons" (ISO27001). This is the only time complexity is mentioned in the standard. However, it indicates that it is vital to remember complexity when coping with systemic complexity in risk management, even though it can be argued that mentioning complexity one time is not good enough.

A consequence of not highlighting complexity more brightly is that organizations with a lack in their risk culture may forget to consider that complexity is a crucial factor when handling systemic complexity in risk management. Moreover, this is what we aim to highlight in this section, that the Norwegian financial sector needs to be more aware of the dangers within a complex system. A system that is so complex can create dangers and risks in the system itself. By not addressing the fact that a system might be complex in a way that might lead to errors, vulnerabilities, and undesirable events, we argue that ISO27001 needs to acknowledge the complexity more comprehensively.

Furthermore, we support the sector's use of NIST and ISO27001 regarding risk management related to cyber events. This is because of a well-formulated standard that is internationally recognized and well-founded. The framework from NIST and the standard ISO27001 might contain sufficient risk descriptions and guidelines.

We endorse the ISO27001 standard as a sound guide to risk management when handling risk in cyber-security. However, we argue that the standard has some flaws in aspects of complexity due to the lack of reviewing the unintended and possible side effects when a system is complex. In our view, the same argument applies to the NIST-framework.

5.3 Why do cyber-threats impact risk, risk analysis and risk management in the financial sector?

It is due for the last sub-question in this thesis. This question concerns why cyber-threats impact the financial sector regarding risk, risk analysis, and risk management, granting us an increased comprehension of how the sector handles the impact of cyber-threats. Without further ado, we aim to present why cyber-threats impact risk, with the involvement and link to risk analysis and management. The risk of this description needs to be well incorporated into risk analysis and management. This means that the financial sector should consider imposed laws and regulations in analysis and management. Further on, confidentiality, access, and integrity in terms of actors becoming a threat will be elaborated.

5.3.1 The impact on the financial sector

As said, there is a gap between the risk and cyber-risk because of the different angles of approaches. Cyber-risk involves, among other things, threats. The connection between cyber-threats, robustness, and resilience is crucial when handling the impact of risk in both analysis and management. In line with the TFM model, the sector must also handle the laws and regulations.

Surely cyber-threats impact risk and how the sector conducts the risk analysis. Aven (2020) defines *risk analysis* as a "systematic process to comprehend the nature of risk and to express the risk, with the available knowledge." However, risk analysis can also be understood more broadly. The SRA defines it as "risk analysis is defined to include risk assessment, risk characterization, risk communication, risk management, and policy relating to risk, in the context of risks of concerns to individuals to public and private sector organizations, and to society at a local, regional, national, or global level." For the financial sector, this means that it needs to consider the cyber-threat in how they perform the assessment, how they characterize it, and policy responses regarding its impact.

Several factors determine why cyber threats are dangerous to the three risk-inclusive points. As mentioned earlier, risk as a concept and definition is difficult to define, making it a situational definition or concept. Based on SRA (2018), there are several definitions, but not a specific one as other researchers claim. This different view of risk can be a weakness in terms of how cyber threats can influence the Norwegian financial sector's perception of cyber-risk. It is not the case that a definition is a weakness in itself. However, since it is difficult to define a concept for researchers, it can be argued that there is a weakness in the concept and may influence how the Norwegian financial sector understands the concept of risk.

Risk analysis is integral to understanding and mapping how different threats can be a risk. Cyber-risk affects the risk analysis because it helps determine what the risk experts believe is necessary to take care of. As mentioned throughout the task, cyber risk is a threat that is constantly evolving, and one never quite knows what to expect when the next attack occurs. This is an essential factor in why cyber threats affect this part of the process. Using standards and frameworks makes it easier for the actors who participate in the risk analysis to conduct a thorough analysis. We have previously, in the thesis, argued that the framework of NIST is not good enough when it comes to the need for a better understanding of complexity. This also helps to weaken confidence in the framework as a tool in this part of the process and should therefore be an essential part that should be included in the risk analysis to understand how this affects further work with the handling in the next part of the process.

The last part of dealing with cyber threats is risk management based on risk and risk analysis. Based on findings in the risk analysis, it should be possible to carry out and implement measures to prevent unauthorized attacks on the Norwegian financial sector. Cyber-risk is also a factor here, as in the previous parts. Several things come into play within risk management, based on which measures are to be implemented. In the risk analysis, the experts have presented their views and provided guidelines for which measures they believe are the most necessary. However, it is not that simple. An important factor that comes into play is finances. In most companies, risk and security is a "post" where you do what is necessary but do not put in large financial sums. When there is a constant risk that a cyber-attack will occur, it is not the case that companies in the Norwegian financial sector invest large sums of money in stopping all attacks, especially when they do not know what to expect. This leads to uncertainty about how to emphasize the risk and decide which measures to implement. Cost-benefit is, therefore, a concept that plays a significant role in risk management. Based on Finanstilsynet's (2021)

analysis, the only thing we know for sure is that there is a risk that will continue at a higher activity level and with more developed methods than now.

However, a successful strategy for managing information security by withstanding and resisting information threats notably affects its further development. It might prove challenging to acknowledge any human activity carried out without digital and computer technology, caused by the growth of information that requires processing and analysis. Furthermore, increased information generates a risk of using information for criminal purposes (Yarovenko, 2020). Throughout this chapter, we acknowledge that the sector always needs to be on its front foot regarding development. The financial sector is a complex sector with multiple systems and components. Rosness et al. (2004) claim redundancy can prevent a system brake down as e result of unwanted events.

5.3.2 Internal actors as an influencing factor

It has been explained earlier in the thesis that employees internally can help increase the risk around privacy information, where accessibility, integrity, and confidentiality play a significant role. Information processing and ICT use are vital tasks for the Norwegian financial sector. If the systems or treatment do not work correctly, it can lead to significant consequences for goals, efficiency, and compliance with laws and regulations. Therefore, internal control plays a significant role in privacy in the sector. Information security is performed well if it contains an adequate and balanced assurance of confidentiality, integrity, and availability of information in the company's information processing. This is because it is not a static condition since threats and risks change quickly and over time, and measures should be systematically adapted with developments.

Access

Regarding accessibility, the management, employees, and external users need continuous and effective access to relevant information, ICT systems, and digital services. Failure to do so can increase the likelihood of wrong decisions, inefficient work, lost work time, errors in financial transactions, and breaches of customers' rights and privacy. It is these consequences securing accessibility that should reduce and eliminate. Therefore, it is essential that the information is authorized when needed (Digdir, n.d.). A valuable tool for reducing accessibility is that access to relevant ICT systems is based on role-based access criteria. Therefore, it is crucial to correct

access rights to various systems in connection with the assignment of new roles, changes in organizations or work tasks, and terminations of employment (UNIT, 2020). In our case, organizations should continuously keep up with employees' requirements and only grant permission for personal information when needed. If a person has a role in an organization and always needs accessibility, that person should always be granted it. The topic is more about reducing access to the set of people necessary to use the information and will be a step in the right direction to reduce the risk of personal data being misused by internal actors.

Integrity

The next point to reduce privacy breaches is if the information has been changed unintentionally or by unauthorized persons, it can be said that it has lost its integrity and the information processing then takes place on the wrong basis. Digdir (n.d.) then says that neither employees nor external actors can rely on information in the best case. We can compare availability and integrity by increasing the likelihood of wrong decisions, inefficient work, lost working time, errors in financial transactions, breaches of customers' rights and privacy, and breaches of integrity. If a hacker gains access to the company's systems and can change the information internally, it will be detrimental to integrity. Such consequences ensure that the integrity of the business should be reduced or eliminated. Hence, the importance of comparing integrity with robustness. Based on Aven et al. (2004) definition of robustness, it is also essential to consider internal influences, like integrity. The reason why integrity is so important is because of the significant damage it could cause the organization.

Confidentiality

Confidentiality is the last factor that plays a role in reducing the risk of privacy breaches in the Norwegian financial sector. This factor comes into play so that the information does not become known to unauthorized persons. Confidentiality concerns the statutory duty of confidentiality or in-company additional guidelines on what is to be exempted from the public. Confidentiality, therefore, has a function that ensures that the information will only be available to those who are to have access to the specific information, and, therefore, unauthorized persons cannot access it. If there is a breach of confidentiality, it can affect individuals, private companies, and the work companies themselves should do. In contrast to the other two points, the consequences of confidentiality will be an uncomfortable feeling, loss of reputation and integrity, a devastating situation, monetary loss, difficulty in carrying out proper case processing, and

disclosures of secrets for the business. That is why securing confidentiality should reduce or eliminate such consequences (Digdir, n.d.).

5.4 Findings

Looking back at the beginning of chapter 5, we introduced figure 4, showing that the trend of cyber-events in Norway is increasing with the assumption of this being only the tip of the iceberg. By showing this, we point out the vulnerabilities connected to cyber-crime because we need to have knowledge considering the latest trends and the rapid development of cyber-attacks to be on our front foot, especially when it comes to being able to keep up with the changes in the way criminal hackers attack. Reports made to inform us about the risk and threats could be argued to be a bit vague, but we are sure that NSM (2018) are right when they claim the trend of digital breaches will further accelerate. Like January 2021, when Østre Toten municipality was exposed to an encryption virus with a ransom demand and the attack on the Norwegian Storting in the autumn of 2020. This shows us the importance of the different actors, with different intentions and ways of performing attacks, which need to be mapped and understood with the correct and current knowledge, to the influencing risk description in the sector.

Not finding a suitable definition of cyber-risk, we choose to make our own definition. We did this by trying to enhance the gap between the expert definition and the threat definition in cyber-risk, and by doing so, we argued the importance of the TFM. This model is a fruitful tool in risk analysis and is a suitable and meaningful model to use when handling cyber-threats because of diverse factors involving cyber-risk factors.

Speaking of factors, based on Perrow and Hollnagel, we introduced complexity and the human factor. We argued for the importance of acknowledging this factor. Using TFM and NAT with the focus on the human factor and the complexity made us aware of how the risk description influenced Norway's financial sector.

Complexity is difficult. This chapter provides an understanding of how risk management handles complexity and systemic complexity. We presented the ISO27001 standard and the NIST-framework to introduce how the sector uses the current representation when it comes to handling cyber-threats. This made us visualize the extent of how vital vulnerability and

uncertainty are in complex systems and that complexity within the system itself might contribute to unforeseen and unintended events. We also acknowledge these difficulties in risk management with the constant changes in threat pictures and new and different actors becoming relevant. Therefore, the NIST-framework and the ISO27001 standard are becoming highly relevant when managing these threats. With that, and throughout the empirical chapter, we need to ask ourselves – why. This is made visible in the last part of chapter 5. In both the analysis and management, the connection between cyber-threats, robustness, and redundancy are essential elements when we look at why impact is of such significance to handling cyber-risk—accompanied by laws and regulations set the stage in risk management. Furthermore, by asking the question "why," we have recognized many factors that need to be considered for the Norwegian financial sector to comprehend cyber-threats. The evidence could lie in the threat picture's continuous change and the complexity within the systems, including internal actors with their distinctive characteristics.

Complexity can be connected to longer chains of values and is a factor that increases risk and could lead to more immense consequences in the financial sector. A connection might be new actors and new technology (NOU 2015:13). Based on this and the empirical chapter, we find that complexity is a low focus point in both the NIST-framework and the ISO standard.

6. Discussion

This chapter presents our empirical findings, which will be accounted for and discussed in relation to the theories presented in chapter 3. Previous research will be included in this chapter, where it is relevant if this research can support our theories and empirical approaches. Like chapter 5, the structure in this chapter will follow the same systematic layout of the design, which means that we will start with the same question regarding the build-up of our sub-questions. This chapter will lead us to the main question which concerns this thesis:

"*Drawing on cyber-attacks, how is the risk of losing personal information handled by Norwegian financial sector?"*

6.1 How does continuous change of cyber-attack influence risk description in the financial sector?

The empirical study shows that the level of threat against the financial sector has been developing tremendously since 2015. New forms of events and threats have been detected every year since 2015. This underlines how widespread and comprehensive cyber-security is. With new actors and ways of attack, it is safe to say that the development in motivation, capability, and the methods used by different actors carrying out attacks, is the biggest threat to the sector.

From the empirical study, there are four features in development that cause reason for worrying and might be expected to influence the sector's risk description. These are:

- Increasing complexity
- Professional actors with resources
- Rapid enlargement of development
- Cluttered and unclear environment

6.1.1 Risk description in the financial sector

Throughout the empirical chapter, we acknowledge the development of cyber-threat within the financial sector. The sector is a complex, high technological system that consists of several components and value chains. LaPorte and Consolini (1991) claim that it is possible to prevent system accidents. These accidents can cause diverse threats, and the functionality should be

intact even if severe unwanted events occur. If a threat is trying to cause harm, the sector should implement a robust and redundant system coping with this unwanted event. In line with Rosness et al. (2004), redundancy can prevent a system from breaking down due to this event and that a system should include several layers of defense. However, making a system with increased security and longer value-chains will, according to Perrow (1984), escalate the complexity.

Redundancy being a key element when answering this question, it is crucial when we elaborate on the multi-layer cyber security in cyber. Although we look at the theory about high-reliability organizations concerning how a treat picture can develop with the involvement of different actors, we point out the importance of redundancy relative to HRO. The complexity, competence, and focus of personnel and the security in the system, on its own or an overlapping function. In reality, this means that if something gives or fails, someone else needs to be capable of taking over, or a component takes over for the failing function in the system. We acknowledge this to NAT, where we notice that this might increase the system's complexity. In the theory of normal accidents, it is claimed that a system with its tight connections and interactions will be exposed to an accident at one point. This can easily be translated to the financial sector due to the complexity of the systems. In line with Perrow (1984), we acknowledge that the advantage redundancy could have in the system could also have the opposite effect. This is because of the increasing systemic complexity of a redundant system.

Our empirical presentation leaves no doubt regarding the challenging development of the threat picture and the new trends of threats faced by the financial sector. The sector is aware of the consequences of this; therefore, it is on alert when it comes to handling these values. With Bouveret (2018) in mind, the organization can handle the consequences of direct and short-term effects, while a breach will likely affect only the organization itself. However, it is possible that an event could lead to other actions in a system, and therefore, the system needs to be able to withstand and readjust. The attack on the municipality in Østre Toten shows us that an attack can provide severe consequences for outside parties, like astray sensitive personal information.

Though able to cope and withstand these attacks, new security measures can explain the innovative methods used to carry out an attack. Engen et al. (2016) claim that a safety measure can be against its purpose because it may lead to actors finding new ways and methods to carry out an attack. This way of thinking is also in line with Abrahamsen et al. (2018) when the effect of one single measure might be considered too high, and overinvestment in new safety measures

might occur. The financial sector needs to be aware of both these theoretical theories when coping with the influence of the description of risk. Throughout our empirical presentation, we acknowledge that this might not be the case. We do not claim that this is easy, but this should be more inclusive in the framework because of the rapid development of cyber-attacks.

Based on our empirical presentation, different circumstances and situations can be used and placed in the TFM. Based on our findings, there are mainly two essential actors that need to be handled by the sector: well-funded organized criminals and foreign states. Among the example of the Russian attack on the Norwegian Storting and criminals attacking the municipality of Østre Toten, the empirical demonstration shows us that the risk of carrying out a succeeding attack has increased. Vulnerabilities connected to technology and complexity due to the development in both actors and environment might cause organizational weaknesses and technology usage. Complex systems with an advanced threat picture and tightly linked systems might make us vulnerable due to the new environments and constant change of new risk descriptions (NOU 2000: 24).

The usage of the TFM can provide evaluations that are unquestionably useful and valuable for the financial sector. In chapter 5.1, we provide information that shows the sector is especially vulnerable to cyber-attacks like Ransomware and Phishing (attachment 2). This is likely because the sector is closely linked to essential values, like money and information. This might explain why the sector encounters an increased threat level and why the development is so rapidly changing in the way of attacks. Boholm et al. (2016) claim that a security perspective influences threat when it has the potential to harm important values and has, therefore, a potential to influence risk description. Vulnerability and threats are influenced by resilience and redundancy. However, new vulnerabilities may occur in new technologies that are meant to enhance resilience. This tight connection between the different elements of values, threats, and vulnerabilities could influence the risk description. In line with robustness, resilience, and redundancy, this makes the usage of TFM so treasured for the sector when handling the cyber-risk.

6.2 How does risk management handle increased systemic complexity?

Improving management and having a robust and resilient system that can withstand cyber-attacks is key to protecting personal data. In chapter 3, we explained risk management based on Hopkins, Aven, Perrow, and Hollnagel's theories on design, execution, and evaluation process. We underline the importance of the NIST-framework and the ISO27001 standard with their representation in the sector as a guide for managing risk, but with a critical deficiency. From the empirical study, there are three features in handling systemic complexity that cause reason for worrying and might be expected to influence the handling of risk management. These are:

- The importance of acknowledging risk and development
- Recognize robustness, resilience, and redundancy
- Enhanced understanding and desire to include systemic complexity

6.2.1 Risk management and systemic complexity

Throughout the empirical, we saw that the risk management process is essential when handling risk. Hopkin stated that it is important to remember that risk management does not have the same meaning in every situation (Hopkin, 2017). To justify this, the constant development in methods and actors means that one should try to keep up with the new trends. Therefore, Hopkin's statement is vastly relevant. Considering that risk management is a concept that was developed in the 1950s, it is a concept that has had to develop over the years. When the development of methods and actors constantly evolves, it is equally essential that the risk management process should also follow this development.

We have already discussed that there is no global agreement between scholars on a definition of the term risk. It also makes it challenging to define risk management. One can look at this from two different views. If one favors this disagreement, you can argue that you can adapt the definition based on the problem you are facing. This gives risk managers the freedom to simplify but specify the definition. However, suppose you are critical of the disagreement among scholars. In that case, you can argue that it may be more likely to include essential parts into account when dealing with risk. We emphasize the definition of Aven (2020) that “risk management is a framework that covers alle measures and activities carried out to manage and govern risk, while balancing developments and exploring opportunities on one hand, while

avoiding losses, accidents, and disasters on the other." This definition provides a reasonable basis where the essential principles are included while also seeing the importance of robustness, resilience, and redundancy. Three vital parts need to be highlighted to improve and secure private information in the Norwegian financial sector.

Digital development makes the Norwegian financial sector more connected to technological systems and contributes to employees and customers having to apply digital processes. The cyber-domain is tightly linked to complex interactions. In chapter 5, redundancy, technology, actors, and the development of methods are factors that can increase the likelihood of complexity within a system. Based on the theory of Hollnagel (2012) presented in chapter 3, complexity is a key to handling cyber-risk in constant development. Specifically, for the ones that are in charge of identifying incoming risks. In the empirical, Brown (2021) makes visible the importance of constant change in threats and the ability to maintain robust systems. Complexity in digital development is the key to staying up to date and maintaining a robust system that can withstand threats and dangers. In the Norwegian financial sector, there is already a high level of complexity in the systems used, but as mentioned earlier, organizations in the Norwegian financial sector use subcontractors. They are responsible for various tasks in their work. These are often companies they do not have a complete overview of, which increases the systemic complexity and could increase weaknesses when cyber-attacks occur.

6.2.2 ISO27001 and the NIST-framework

We have placed much emphasis on the framework of NIST through this assignment. It is a framework well developed and used globally in the financial sector, including the Norwegian one. The framework's design gives risk managers a clear guide when dealing with risk and is a tool that we believe is professionally strong and well-structured. However, there is a significant weakness within this framework. Through the empirical work, we have emphasized the complexity and importance of including the use of this concept when dealing with risk. In the framework of NIST, not enough focus has been placed on complexity.

To provide a service that can grant secure storage and use of personal information, companies in the Norwegian financial sector should include systemic complexity at the same time as they should include complexity in their work. The TMI accident, explained in chapter 3, is a sound example of how an accident breaks down an entire system and the massive consequences it

might cause. Systemic complexity, with the definition of complexity by SRA (2018) presented in chapter 3, highlights the importance of including it as a strategic base to reduce the probability that this will occur in the Norwegian financial sector. The NIST-framework and the ISO27001 standard have chosen not to include it as highlighted chapters through their latest releases, which we see as a significant weakness. Complexity is the key to trying to follow progress with the development of attacks from unknown actors who use constantly evolving methods. Therefore, companies in the Norwegian financial sector should include complexity, even if it is not included in the current framework and standard.

6.3 Why do cyber-threats impact risk, risk analysis and risk management in the financial sector?

This chapter consists of an essential question on why cyber-threats have an impact is has in the sector. We elaborate on the question of risk and the importance of digital development in the financial sector. We understand and underline the importance of knowledge in the development and the implications of complexity. We acknowledge that both the NIST-framework and the ISO27001 standard focus on speedy development, yet again, still need to be more focused on complexity. We mainly find four features from the empirical study that need to be debated. These are:

- Agree upon one definition of risk
- Keep up with digital development
- Implementation of complexity
- Improve internal overview

6.3.1 Risk definition and complexity

The empirical chapter saw the sub-question considering theories and relevant documents. The concept of risk is a concept that needs to get a worldwide agreement on its definition to be capable of agreeing on its importance fully and which elements should be implemented in it. We based the understanding of risk on Aven (2020), which includes systemic process and available knowledge. These are two crucial factors to fully understanding the concept of risk. We argued in chapter X that the definition of cyber-threat was too weak, and we produced our definition based on Oladimeji (2006) and Aven (2020). It could be possible to do the same thing with the definition of risk. However, it is a more compound and complex definition, and we suggest further research is necessary to clarify why cyber risk impacts financial sector risk. The

risk analysis process is also impacted by cyber-risk in the Norwegian financial sector. It impacts this process the most through digital evolution and constant development. The NIST-framework and the ISO27001 standard focus on this rapid development and may be a significant key to success when handling cyber-attacks and personal information.

To comprehensively analyze risk in the Norwegian financial sector, the NIST-framework and ISO27001 standard should implement complexity as the primary point in their "recipes" to reduce the risk of cyber-attacks. Hollnagel (2012) claims that the solution regarding complexity is to stop solving problems one by one with new designs or more powerful technology but instead understand how joint systems achieve their requisite dynamic stability and how they can support this essential capability. His description of complexity is vital to understanding and explaining why the cyber-risk impacts the risk analysis process in the Norwegian financial sector. Therefore, they should include complexity in their risk analysis process and "out-run" the NIST-framework and the ISO27001 standard. This would improve their routines and ensure private information more appropriately.

6.3.2 Digital development and internal issues

Based on Finanstilsynet (2021), we can assume that cyber-attack trends will increase over the years, and measures concerning risk management should be prioritized with high severity. As Aven (2020) states, this part of the process should be prioritized since it is a framework that covers all measures and activities carried out to manage and govern risk while at the same time balancing developments and exploring opportunities on the one hand while avoiding losses, accidents, and disasters on the other. The whole process of deciding which measures to implement is decided in this part and is greatly affected by cyber-threats. Cost-benefit is briefly explained chapter 5.3.1 and is what we believe to be one of the most decisive factors when managing risk. If measures implemented in the past do not turn out to be suitable, it may be that in the following times, they choose to reduce security costs and instead act when an attack occurs. We recognize this, but we do not believe this to be good management. To maintain a safe Norwegian financial sector, with a focus on securing personal information, sufficient financial resources should be set aside to keep up with the risk.

Charles Perrow (1984) explains in his NAT that it is common and natural that accidents occur but does not focus enough on internal actors as one of the main factors for an accident to arise.

Internal actors are an influencing factor and go hand in hand with NAT. NSM´s (2022) latest report highlights the importance of recognizing this as a high vulnerability for companies. Access, integrity, and confidentiality could be fundamental aspects when companies in the Norwegian financial sector try to decrease cyber-attacks, even though the sector in some way has been forced to acknowledge this with the implementation of new laws and regulations. With this chapter in mind, it is time to conclude this thesis.

7. Conclusion

This is the last and conclusive chapter of this thesis, and the question at hand gives us the chance of multiple answers. However, there is a clear and observable relation between compound connections on how the risk of losing personal information is handled. We need to provide knowledge on the fact that the risk needs to be seen in correlation with different factors and reasons. We lay out varied reasons for what we see as being of particular importance, and even though the cyber-threat has increased with the association of awareness and reducing measures in the sector, the following is to be seen as our main finding towards a more united way of handling personal information.

Our main findings are:

- **Implementation and enactment of complexity in existing material**: Even though complexity is mentioned in both the framework and standard, it is nowhere near enough to cope with the importance of this factor. This increases the cyber-risk in the sectors systems and organizations with the development of long and complex chains. In addition, unwanted events represent an increasing total cyber-risk. This is made by cyber-threats and cyber-dangers. Therefore, the TFM is important if we look at risk from this perspective.

- **Speedy development and an arduous environment**: Cyber-risk has developed because of digitalization in the sector. This makes the sectors' values accessible, and the development is sped up by innovation and new technology. However, actors with the intention of causing harm may adjust their methods according to the implementation of measures taken by the sector. It can also be claimed that the

actors are finding new ways of causing harm before the measures implemented by the sector are up to date.

- **Endorsement of robustness, relicense and redundancy:** Vulnerability should be seen in relation to the development in threats and risk. With the laws and regulations, the current framework and standard, displays that there is less vulnerability in technology today than before. This has a positive effect on cyber-risk. By these regulations, the sector has been made aware of the risks, and then taken measures to cope with the cyber-risk. Especially, the new GDPR law made this visible throughout the sector.

The Norwegian financial sector should take responsibility for including the importance of complexity in dealing with breaches of private information. Hollnagel (2012) claims complexity needs to be more incorporated, but this should be included in a better way than it is today. If so, the sector will be better equipped to handle attacks on their company and systems. In addition, resilience, redundancy, and robustness are three essential factors that come into play. They help to measure how the companies manage to resist attacks, at the same time as they help to see how the companies tend to recover systems that are exposed to attacks by known or unknown actors. The consequences of an unintended event have increased and led to a higher risk of cyber-threats that heighten the total cyber-risk. The relevance is exceptionally high when we see risk through the TFM, with value, threat, and vulnerability as crucial factors alongside the B type of knowledge by Aven (2017).

Throughout this thesis, in the theory chapter and our empirical validation, we have tried to perceive how the Norwegian financial sector handles breaches when handling private information. It is a large and complex problem with long value chains that can be most difficult to deal with once it occurs, and the consequences can be significant and worthy of attention. However, it might be a problem that can be dealt with by introducing measures and keeping up with laws and guidelines. The Norwegian financial sector should be aware of the rapid digital developments and new ways of attack. New actors, both criminals, and states. Internal actors are an influencing factor and go hand in hand with NAT. Perrow (1984) claims that we need to acknowledge the factor of internal actors with rising complexity as one of the main reasons for accidents. Additionally, we can only assume that the trend of cyber-attacks will increase.

One solution to dealing with privacy breaches is by following the framework of NIST, at the same time as they should be based on the ISO27001 standard. In addition, the work should be done following the current laws and regulations. The regulations, framework, and standard are well-developed tools that will help reduce the likelihood of personal information going astray. Internationally recognized and solid theories increase the understanding of security, and the risks that follow this subject will help the sector cope with the complex scene of cyber-risk.

Our main argumentation is that when we conclude the risk of losing personal information in the Norwegian financial sector, we would recommend that the sector include complexity more extensively when handling personal information. Suppose they do not include complexity more sufficiently, in that case, we argue that the Norwegian financial sector does not take the importance of storage and handling of personal data in all seriousness. Also, this goes for the inclusion of complexity in the NIST-framework and ISO27001 standard more comprehensively and diversely than today. This is something that we acknowledge as particularly important and might be the difference in how the sector succeeds in its work against cyber-crime.

The framework and standards should be more connected with complexity because of the long value chains, rapid development, and cluttered environments, which all contribute to an overall higher cyber-risk when handling personal data.

This thesis has unveiled some challenges connected to cyber-risk and handling personal information. As a result, we encourage further research on the development and digitalization of the Norwegian financial sector. We become aware of a better way of implementing complexity in both the current framework and standard. There is a need to investigate how complexity could be better applied and acknowledged. From a risk expert's view, it is essential to strive for a better understanding and implementation of complexity, even though this might come with pros and cons.

It is likely that something unlikely will happen (Aristoteles, 284 – 322 BC.)

8. Bibliography

Abrahamsen, E. B., Moharamzadeh, A., Abrahamsen, H. B., Asche, F., Heide, B., Milazzo, M. F. (2018). *Are too many safety measures crowding each other out.* https://doi.org/10.1016/j.ress.2018.02.011

Aion Digital. (2020, November 3). *The Short History of Fintech.* https://aiondigital.com/the-short-history-of-fintech/

Aven, T., Boyesen, M., Njå, O., Olsen, K.H. & Sandve, K. (2004). *Samfunnssikkerhet*. Universitetsforlaget.

Apple. (2022). *Apple Pay.* Retrieved from https://www.apple.com/no/apple-pay/

Aven, T. (2017). An Emerging New Risk Analysis Science: Foundations and Implications. Risk Analysis 38(7). https://doi.org/10.1111/risa.12899

Aven, T. (2019). The cautionary principle in risk management: Foundation and practical use. *Reliability Engineering & System Safety, 191*, 106585. https://doi.org/10.1016/j.ress.2019.106585

Aven, T. (2020). *The Science of Risk Analysis.* (1nd ed.) Routledge.

Bannigan, K., & Watson, R. (2009). Reliability and validity in a nutshell. *Journal of Clinical Nursing.* 18, 3237–3243. https://doi.org/10.1111/j.1365-2702.2009.02939.x

Bellamy, A.M., & Berg, F.R. (2019, December 18). *Rapportering av IKT-hendelser til Kredittilsyn.* Finanstilsynet. Retrieved from https://www.finanstilsynet.no/nyhetsarkiv/rundskriv/2009/rapportering-av-ikt-hendelser-til-kredittilsynet/

Boholm, M., Moller, N., Hansson, S. E. (2016). *The concept of risk, safety, and security: applications in everyday language.* Risk Analysis. 36(2), 320-338. https://doi.org/10.1111/risa.12464

Bouveret, A. (2018). *IMF working paper: Cyber Risk for the Financial Sector: A framework for Quantitative assessment.* Retrieved from https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924

Bowcut, S. (2021, February 25). *Cybersecurity in the financial services industry.* Cybersecurity guide. Retrieved from https://cybersecurityguide.org/industries/financial/

Bowen, G.A. *(2009).* Document Analysis as a Qualitative Research Method. *Qualitative Research Journal.* 9(2). 27-40. https://doi.org/10.3316/QRJ0902027

Bradford, A., Weisberger, M. (2021, December 7). *Deductive reasoning vs. Inductive reasoning.* Live Science. Retrieved from *https://www.livescience.com/21569-deduction-vs-induction.html*

Brown, L. (2021). *What is Risk Management in Project Management?*. Retrieved from https://www.invensislearning.com/blog/risk-management-in-project-management/

Busmundrud, O., Maal, M., Kiran, J.H., & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger.* (FFI-rapport 00923). Forsvarets forskningsinstitutt. https://publications.ffi.no/nb/item/asset/dspace:2503/15-00923.pdf

Chartered Financial Analyst Institute. (2022). *Systemic Risk & Management in Finance.* Retrieved from https://www.cfainstitute.org/en/advocacy/issues/systemic-risk#sort=%40pubbrowsedate%20descending

Digitaliseringsdirektoratet. (n.d.). *Hvorfor styring av informasjonssikkerhet?*. Retrieved from https://www.digdir.no/informasjonssikkerhet/hvorfor-styring-av-informasjonssikkerhet/3145

Digitaliseringsdirektoratet b. (n.d.). *Kva seier NS-ISO/IEC 27001?*. Retrieved from https://www.digdir.no/informasjonssikkerhet/kva-seier-ns-isoiec-27001/3060

Doe, C. (n.d). *Cybersecurity In Financial Services.* EY. Retrieved from *https://www.ey.com/en_gl/innovation-financial-services/cybersecurity*

Dudovskiy, J. (2016). *The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance.* (6nd ed). Research Metodology Net.

Ekberg, E., & Vatnaland, J. (2003). *Strukturendring i norsk finanssektor*: Fragmentering, makt og styringsavmakt i skjæringspunktet mellom næringsliv og politikk. Makt- og demokratiutredningens rapportserie, ISSN 1501-3065. https://www.sv.uio.no/mutr/publikasjoner/rapporter/rapp2003/rapport72/index-4_1.html?fbclid=IwAR2cYjYstVEMs6_nC_8G_0MfOCsGipuXiIm85nYhztUb6QLewRCWVvwvr4Y

Elmaghraby, Adel. S., Losavio, Michael. M. 2014. *Cyber security challenges in Smart Cities: Safety, security and privacy.* https://doi.org/10.1016/j.jare.2014.02.006

Engen, O. A. H., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E. & Pettersen, K. A. (2016). *Perspektiver på samfunnssikkerhet.* Cappelen Damm Akademisk.

European Commission (2021). *Digital Economy and Society Index (DESI) 2021*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/desi

EØS-notatbasen. (2016). *NIS-direktivet.* Retrieved from https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/

Finanstilsynet. (2009). *Rapportering av IKT-hendelser til Kredittilsynet.* Finanstilsynet. Retrieved from *https://www.finanstilsynet.no/nyhetsarkiv/rundskriv/2009/rapportering-av-ikt-hendelser-til-kredittilsynet/*

Finanstilsynet. (2021). *Risiko- og sårbarhetsanalyse (ROS).* Retrieved from https://www.finanstilsynet.no/contentassets/98a84484055840fc8bfd0cb7b78dd025/ros-2021.pdf?fbclid=IwAR34ThylJ0BvveVzKQImbXmp6iGFMtxhHReUBI8dv0_g7evPkArXDjsbWVQ

Fortinet. (n.d.). *Types of Cyber Attacks.* Retrieved from https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

Gartner. (n.d.) *Gartner Glossary.* Retrieved from https://www.gartner.com/en/information-technology/glossary/digitalization

Herrman, H., Stewart, D. E., Diaz-Granados, N., Berger, E. L., Jackson, B., Yuen, T. (2011). *What Is Resilience?* https://doi.org/10.1177/070674371105600504

Hollar, M., Giffen, B. V., Benzell, S., & Ehrat, M. (2020). *The General Data Protection Regulation in Financial Services Industries: How Do Companies Approach the Implementation of the GDPR and What Can We Learn From Their Approaches.* Retrieved from https://www.researchgate.net/publication/340003405_The_General_Data_Protection_Regulation_in_Financial_Services_Industries_How_Do_Companies_Approach_the_Implementation_of_the_GDPR_and_What_Can_We_Learn_From_Their_Approaches

Hollnagel, E. (2008). *The Changing Nature of Risks.* Ergonomics Australia Journal, 2008, 22 (1-2), pp.33-46. Retrieved from https://www.researchgate.net/publication/45514196_The_Changing_Nature_of_Risks

Hollnagel, E. (2012). *Coping with complexity: Past, present and future.* Cognition Technology and Work 14(3). https://doi.org/10.1007/s10111-011-0202-7

Hopkin, P. (2017). *Fundamentals of Risk management: Understanding, evaluating and implementing effective risk management* (4nd ed). Kogan Page Limited. http://dspace.vnbrims.org:13000/xmlui/bitstream/handle/123456789/5077/Fundamentals%20of%20Risk%20Management.pdf?sequence=1

Hopkins, A. (2002). Was Three Mile Island a 'Normal Accident'?. *Journal of Contingencies and crisis management.* 9(2). 65-72. https://doi.org/10.1111/1468-5973.00155

Horvath, I. (2021, 17. July) *Five Steps of Risk Management Process.* Retrieved from https://www.invensislearning.com/blog/risk-management-process-steps/
https://nsm.no/hold-deg-oppdatert/meninger/digitale-trusler-i-2021
https://o.nsd.no/arkivering/sikkerhet_og_vedlikehold.html

Hægeland, T., & Kongsrund P.M. (2019, October 10). *Norges Bank og Finanstilsynet ber om innspill til evt. innføring av rammeverk for testing av cybersikkerhet i Norge.* Norges Bank. Retrieved from https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Brev-og-uttalelser/2019/2019-10-10-naeringen/

ISO. (2018). *ISO 31000:2018(en). Risk management — Guidelines*. Retrieved from https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

Johannesen, A., Christoffersen, L., & Tufte, P. A. (2011). *Forskningsmetode for økonomiskadministrative fag* (3nd ed). Abstrakt forlag.

Kommunal- og distriktsdepartementet (2019, 30. October). Ny personopplysningslov. Retrieved from https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/ny-personopplysningslov/id2340094/

Kruse, C. S., Frederick, B., Jacobson, T., & Monticon, K. D. (2017). Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends. Technology and health care, vol. 25, no. 1, pp. 1-10, 2017. DOI: 10.3233/THC-161263

Lagazio, M., Sherif, N., & Cushman, M. (2014). *A multi-level approach to understanding the impact of cyber crime on the financial sector.* Computers & Security. Volume 45, September 2014, Pages 58-74. https://doi.org/10.1016/j.cose.2014.05.006

La Porte, T., Consolini P.M. (1991). Working in Practice Byt Not in Theory: Theoretical Challenges of «High Reliability Organizations». *Journal of Puclic Administration Research and Theory, 1*(1), 19-48. Retrieved from https://www.jstor.org/stable/1181764

Le Coze, J. C. (2020). *Post Normal Accident* (1nd ed). CRS Press

Malt, U., & Tjernshaugen, A. (2020, July 18). K*valitativ.* Store Norske Leksikon. Retrieved from https://snl.no/kvalitativ

Martinussen, L.C. (2022, February 24). Danske Bank rammet av svindel: Kraftig advarsel:- Urovekkende!. *Dagbladet, Børsen.* https://borsen.dagbladet.no/nyheter/kraftig-advarsel-urovekkende/75462573

Næringslivets Handlesorganisasjon. (n.d.) *Digitalisering.* Retrieved from https://www.nho.no/publikasjoner/p/naringslivets-perspektivmelding/digitalisering/

Nasjonal Sikkerhetsmyndighet. (n.d.) *Ofte stilte spørsmål om Grunnprinsipper for IKT-sikkerhet.* Retrieved from https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/informasjon-om-nsms-grunnprinsipper-for-ikt-sikkerhet/

Nasjonal Sikkerhetsmyndighet. (2018). *Risiko 2018: Verdifulle individer, verdifull infrastruktur, verdifulle virksomheter*. Retrieved from *https://nsm.no/getfile.php/133720-1592915838/Filer/Dokumenter/Rapporter/nsm_risiko_2018_web.pdf*

Nasjonal Sikkerhetsmyndighet. (2021). *Nasjonalt digitalt risikobilde 2021.* Retrieved from *https://nsm.no/getfile.php/137495-1635323653/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf*

Nasjonal Sikkerhetsmyndighet. (2022). *Risiko 2022: Økt risiko krever økt årvåkenhet.* Retrieved from https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

NIST (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

NOU 2000: 24. (2000). *Et sårbart samfunn — Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Justis- og beredskapsdepartementet. Retrieved from https://www.regjeringen.no/no/dokumenter/nou-2000-24/id143248/

NOU 2015: 13. (2015). *Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Justis- og beredskapsdepartementet. Retrieved from https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

NOU 2018: 14 (2018). *IKT-sikkerhet i alle ledd — Organisering og regulering av nasjonal IKT-sikkerhet.* Justis- og beredskapsdepartementet. Retrieved from *https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/?ch=2*

NTNU. (n.d.). *Informasjonssikkerhet- risikovurdering.* Retrieved from https://i.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+risikovurdering

Oladimeji, E.A., Supakkul, S., & Chung, L. (2006). *Security threat modeling and analysis: A goal-oriented approach.* Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?

Perrow, C. (1984). *Normal Accidents – living with high risk technologies.* Basic books

Politiets sikkerhetstjeneste. (2021). *National Threat Assessment 2021.* Retrieved from https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/download-the-national-threat-assessment-2021-in-english.pdf

Reason, J. (1997). Managing the Risks of Organizational Accidents. Hampshire: Ashgate Publishing Limited.

Ridderstrøm, H. (2021, 16. April). *Bibliotekarstudentens nettleksikon om litteratur og medier.* Retrieved from *https://www.litteraturogmedieleksikon.no/gallery/litteraer_analyse.pdf*

Rosa, E.A., Renn, O., & McCright, A.M. (2014). The Risk Society Revisited: Social Theory and Governance. *American Journal of Sociology.* 120(5). 1565-1567. https://doi.org/10.1086/679653

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R.K., & Herrera, I.A. (2004). *Organisational accidents and resilient organisations : five perspectives*. Retrieved from https://bibsys-almaprimo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=BIBSYS_ILS71494542870002201&context=L&vid=UBIS&lang=no_NO&search_scope=default_scope&adaptor=Local%20Search%20Engine&isFrbr=true&tab=default_tab&query=isbn,contains,8214027241,AND&mode=advanced

Røv, S. A. (n.d.) *Informasjonssikkerhet – risikovurdering.* Retrieved from https://i.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+risikovurdering

Royal Literary Fund. (n.d.). *What is a literature review?*. Retrieved from https://www.rlf.org.uk/resources/what-is-a-literature-review/

Schwarcz, S. L. (2008). Systemic Risk. *The Georgetown Law Journal.* 97(1). 193-251. Retrieved from https://articleworks.cadmus.com/geolaw/zt100109.html

Skjelvik, A. (2019). *Cyber-risiko i den norske finanssektor.* [Master's degree, University of Stavanger]. Uis.brage.unit. https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/2628889/Skjelvik_Alvhild.pdf?sequence=1&isAllowed=y&fbclid=IwAR3OtC_O9QgKhrnP4n4vP8S3JAP6aSfT8vELjYPBSuXPMLkWMvEDfYxSpeM

Sobers, R. (2021, March 16). *134 Cybersecurity Statistics and Trends for 2021*. Varonis. Retrieved from https://www.varonis.com/blog/cybersecurity-statistics

SRA. (2018). *Society for Risk Analysis Glossary*. Retrieved from https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

Standard Norge. (2022, May 23). *Ledelsessystemer for informasjonssikkerhet - Krav – NS-EN ISO/IEC 27001.* Retrieved from https://www.standard.no/fagomrader/ikt/it-sikkerhet/isoiec-27001/

Stine, K., Quinn, S., Witte, G., & Gardner, R.K. (2020). *Integrating Cybersecurity and Enterprise Risk Management (ERM).* https://doi.org/10.6028/NIST.IR.8286

Tang, A. (2020, 30 June). Privacy Risk Management. *ISACA Journal.* Vol 4. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/privacy-risk-management

Tjora, A. (2021). *Kvalitative forskningsmetoder i praksis.* 4th edition. Gyldendal.

Unit. (2020). *Informasjonssikkerhet og personvernforordningen (GDPR).* Unit. Retrieved from *https://www.unit.no/informasjonssikkerhet-og-personvernforordningen-gdpr?fbclid=IwAR21uWYFZGBHrKwU5M_RGirMaviyZb5XOeP00C0MFj1pAvk2yuhFg6zSvPs*

Universitetet i Oslo. (2010). *Historisk bakgrunn- utvikling i finanssektoren.* Retrieved from https://www.sv.uio.no/mutr/publikasjoner/rapporter/rapp2003/rapport72/index-4_1.html?fbclid=IwAR2Ictf8Lqxduj8dsgl9VXCTnUKFh_G9Y4o55zEayVprDF_4wy4IAuay1y4

University of Edinburgh. (2022). *Literature review.* Retrieved from https://bibsys-almaprimo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=BIBSYS_ILS71544765140002201&context=L&vid=UBIS&lang=no_NO&search_scope=default_scope&adaptor=Local%20Search%20Engine&isFrbr=true&tab=default_tab&query=any,contains,Introduksjon%20til%20samfunnsvitenskapelig%20metode&offset=0

Visma. (n.d.) *Why is cyber security important?* Retrieved from https://www.visma.com/cyber-security/why-is-cyber-security-important/

World Economic Forum (2022). *The Global Risks Report 2022.* (17nd ed). Retrieved from *https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf*

Yarovenko, H. (2020). *Evaluating the threat to national information security.* Volume 18 2020, Issue 3. 195-210.
http://dx.doi.org/10.21511/ppm.18(3).2020.17

Attachments

Attachment 1: The Security Act (Sikkerhetsloven)

In our thesis we focus on the Norwegian Financial sector which particularly play an important role for the maintenance of key societal functions and in addition, handles personal information on an everyday basis. The Norwegian Financial sector is obliged to follow this law.

Norway's new Security Act entered into force on 1 January 2019 and replaced the previous Act on Preventive Security Services. The rules of the Security Act apply as a starting point to enterprises that are covered by the scope of the Act.

One of the significant changes with the new law was the rules on ownership control, i.e., rules on duty to notify and approve a qualified ownership interest in companies subject to the law.

Note: the notification obligation only applies where the target company is subject to the law pursuant to a so-called § 1-3 decision (see third bullet point below).

Which businesses are covered?

- State, county, and municipal bodies.
- Suppliers of goods or services connected with security-graded procurements by Chapter 9 of the Act (see definition below).
- A security-graded procurement means that the product or service supplier can access or manufacture security-graded information or gain access to an object or infrastructure worthy of protection.
- Assumes that a security agreement has been entered.
- Enterprises that by decision (§1-3) have been subject to the rules of the Security Act (in whole or in part).
- Businesses that may be subject to it must be notified in advance of any decision. If you have not received notification of such a decision, you can assume that you are not covered.
- The authorities will also be able to intervene in connection with acquisitions of companies that are not explicitly covered by the scope of the Security Act.

Attachment 2: Types of cyber-attacks (Based on Fortinet, n.d.)

- Birthday Attack

In a birthday attack, an attacker abuses a security feature: hash algorithms, which are used to verify the authenticity of messages. The hash algorithm is a digital signature, and the receiver of the message checks it before accepting the message as authentic. If a hacker can create a hash that is identical to what the sender has appended to their message, the hacker can simply replace the sender's message with their own. The receiving device will accept it because it has the right hash.

- Brute force attack

A brute-force attack gets its name from the "brutish" or simple methodology employed by the attack. The attacker simply tries to guess the login credentials of someone with access to the target system. Once they get it right, they are in.

- DNS Spoofing

With Domain Name System (DNS) spoofing, a hacker alters DNS records to send traffic to a fake or "spoofed" website. Once on the fraudulent site, the victim may enter sensitive information that can be used or sold by the hacker. The hacker may also construct a poor-quality site with derogatory or inflammatory content to make a competitor company look bad.

- DoS and DDoS Attacks

A denial-of-service (DoS) attack is designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests. A distributed denial-of-service (DDoS) attack is similar in that it also seeks to drain the resources

of a system. A DDoS attack is initiated by a vast array of malware-infected host machines controlled by the attacker. These are referred to as “denial of service” attacks because the victim site is unable to provide service to those who want to access it.

- Drive-by Attacks

In a drive-by attack, a hacker embeds malicious code into an insecure website. When a user visits the site, the script is automatically executed on their computer, infecting it. The designation “drive by” comes from the fact that the victim only has to “drive by” the site by visiting it to get infected. There is no need to click on anything on the site or enter any information.

- Eavesdropping Attacks

Eavesdropping attacks involve the bad actor intercepting traffic as it is sent through the network. In this way, an attacker can collect usernames, passwords, and other confidential information like credit cards. Eavesdropping can be active or passive. With active eavesdropping, the hacker inserts a piece of software within the network traffic path to collect information that the hacker analyzes for useful data. Passive eavesdropping attacks are different in that the hacker “listens in,” or eavesdrops on the transmissions, looking for useful data they can steal.

- Insider Threats

People within a company’s own doors pose a special danger because they typically have access to a variety of systems, and in some cases, admin privileges that enable them to make critical changes to the system or its security policies. In addition, people within the organization often have an in-depth understanding of its cybersecurity architecture, as well as how the business reacts to threats. This knowledge can be used to gain access to restricted areas, make changes to security settings, or deduce the best possible time to conduct an attack.

- Malware attacks

Malware is a general term for malicious software, hence the “mal” at the start of the word. Malware infects a computer and changes how it functions, destroys data, or spies on the user or network traffic as it passes through. Malware can either spread from one device to another or remain in place, only impacting its host device. Several of the attack methods described in this section can involve forms of malware, including MITM attacks, phishing, ransomware, SQL injection, Trojan horses, drive-by attacks, and XSS attacks.

- MITM Attacks

Man-in-the-middle (MITM) types of cyber-attacks refer to breaches in cybersecurity that make it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers. It is called a “man in the middle” attack because the attacker positions themselves in the “middle” or between the two parties trying to communicate. In effect, the attacker is spying on the interaction between the two parties.

- Password Attack

Passwords are the access verification tool of choice for most people, so figuring out a target’s password is an attractive proposition for a hacker. This can be done using a few different methods. Often, people keep copies of their passwords on pieces of paper or sticky notes around or on their desks. An attacker can either find the password themselves or pay someone on the inside to get it for them.

- Ransomware attacks

With ransomware, the victim’s system is held hostage until they agree to pay a ransom to the attacker. After the payment has been sent, the attacker then provides instructions regarding how the target can regain control of their computer. The name "ransomware” is appropriate because the malware demands a ransom from the victim.

- Session Hijacking

Session hijacking is one of multiple types of MITM attacks. The attacker takes over a session between a client and the server. The computer being used in the attack substitutes its Internet Protocol (IP) address for that of the client computer, and the server continues the session without suspecting it is communicating with the attacker instead of the client. This kind of attack is effective because the server uses the client's IP address to verify its identity. If the attacker's IP address is inserted partway through the session, the server may not suspect a breach because it is already engaged in a trusted connection.

- Phishing

A phishing attack occurs when a malicious actor sends emails that seem to be coming from trusted, legitimate sources to grab sensitive information from the target. Phishing attacks combine social engineering and technology and are so-called because the attacker is, in effect, “fishing” for access to a forbidden area by using the “bait” of a seemingly trustworthy sender.

To execute the attack, the bad actor may send a link that brings you to a website that then fools you into downloading malware such as viruses or giving the attacker your private information. In many cases, the target may not realize they have been compromised, which allows the attacker to go after others in the same organization without anyone suspecting malicious activity.

- Spear-phishing

Spear phishing refers to a specific type of targeted phishing attack. The attacker takes the time to research their intended targets and then write messages the target is likely to find personally relevant. These types of attacks are aptly called “spear” phishing because of the way the attacker hones in on one specific target. The message will seem legitimate, which is why it can be difficult to spot a spear-phishing attack.

- SQL Injection Attack

Structured Query Language (SQL) injection is a common method of taking advantage of websites that depend on databases to serve their users. Clients are computers that get information from servers, and an SQL attack uses an SQL query sent from the client to a database on the server. The command is inserted, or "injected", into a data plane in place of something else that normally goes there, such as a password or login. The server that holds the database then runs the command and the system is penetrated.

If an SQL injection succeeds, several things can happen, including the release of sensitive data or the modification or deletion of important data. Also, an attacker can execute administrator operations like a shutdown command, which can interrupt the function of the database.

- Trojan Horses

A Trojan horse attack uses a malicious program that is hidden inside a seemingly legitimate one. When the user executes the presumably innocent program, the malware inside the Trojan can be used to open a backdoor into the system through which hackers can penetrate the computer or network. This threat gets its name from the story of the Greek soldiers who hid inside a horse to infiltrate the city of Troy and win the war. Once the "gift" was accepted and brought within the gates of Troy, the Greek soldiers jumped out and attacked. In a similar way, an unsuspecting user may welcome an innocent-looking application into their system only to usher in a hidden threat.

- URL Interpretation

With URL interpretation, attackers alter and fabricate certain URL addresses and use them to gain access to the target's personal and professional data. This kind of attack is also referred to as URL poisoning. The name "URL interpretation" comes from the fact that the attacker knows the order in which a web-page's URL

information needs to be entered. The attacker then “interprets” this syntax, using it to figure out how to get into areas they do not have access to.

To execute a URL interpretation attack, a hacker may guess URLs they can use to gain administrator privileges to a site or to access the site’s back end to get into a user’s account. Once they get to the page they want, they can manipulate the site itself or gain access to sensitive information about the people who use it.

- Web Attacks

Web attacks refer to threats that target vulnerabilities in web-based applications. Every time you enter information into a web application, you are initiating a command that generates a response. For example, if you are sending money to someone using an online banking application, the data you enter instructs the application to go into your account, take money out, and send it to someone else’s account. Attackers work within the frameworks of these kinds of requests and use them to their advantage.

- Whale-phishing Attacks

A whale-phishing attack is so-named because it goes after the “big fish” or whales of an organization, which typically include those in the C-suite or others in charge of the organization. These individuals are likely to possess information that can be valuable to attackers, such as proprietary information about the business or its operations.

- XSS Attacks

With XSS, or cross-site scripting, the attacker transmits malicious scripts using clickable content that gets sent to the target’s browser. When the victim clicks on the content, the script is executed. Because the user has already logged into a web application’s session, what they enter is seen as legitimate by the web application. However, the script executed has been altered by the attacker, resulting in an unintended action being taken by the “user.”